Harvard University

Privacy in the Internet Age:

Analyzing Federal Legislative Proposals to Enact a Comprehensive Non-Industry-Specific Privacy Regime in the United States

Andrew Farquharson

Policy Analysis Capstone

In Partial Fulfillment of the Requirements for a Master's in International Relations

May 8, 2019

Table of Contents

Executive Summary

Americans today live in the internet age, where mobile devices, the internet of things, social media, ecommerce, and the like provide consumers with new and innovative products and services that make life easier. The proliferation of these same technologies has allowed companies to collect, use, store, share, and sell more information about consumers than ever before. While these activities are necessary to provide consumers with their desired products and services, many of the largest companies, often colloquially referred to as tech giants, have historically been dismissive of Americans' constitutional right to privacy, lying to and deceiving consumers in order to collect as much information possible for self-aggrandizement. While the agency tasked with protecting consumers' privacy, and against unfair and deceptive business practices, issues and limitations within the Federal Trade Commission (also the "Commission," "FTC") have led to a less-than-optimal enforcement record.

While Congress has previously passed legislation in order to protect Americans and their privacy, such legislation is industry-specific and was passed in a time when today's internet was more science fiction than reality. Fearful of stifling innovation, lawmakers have refrained from attempting to regulate the internet sector in its entirety, opting instead for industry self-regulation. It is self-regulation that has allowed tech giants to act as what (UK) Parliament has referred to as "digital gangsters," believing themselves to be ahead of and beyond the law.[1] However, the recent onslaught of data breaches and revelations about the data practices of these companies has caused both Congress and the public to say enough is enough and call for a Federal privacy framework.

Using evaluative criteria developed through the case studies presented in this report's background section and recommendations made by FTC, privacy experts, and White House staff, this report analyzes five legislative proposals put forth by members of Congress seeking to establish a non-industry-specific privacy framework. The evaluative criteria require that an effective framework must:

1. Provide for a Federally-overseen auditing/reporting mechanism wherein companies report on their data and privacy practices to FTC;
2. improve transparency for consumers regarding companies' data and privacy practices;
3. promulgate baseline data/information principles that companies are must abide by;
4. grant FTC Administrative Procedure Act rulemaking authority;
5. allow FTC to assess civil penalties for first-time violators of the frameworks' regulations; and
6. address staffing and funding issues within FTC.

As the only proposal evaluated to address all six of the above criteria, this report recommends the adoption of Sen. Wyden's (D-OR) Consumer Data Protection Act.[2] In addition to these criteria, the Act: utilizes a scope that protects small businesses and start-ups from regulatory overburden, focusing instead on tech giants; acknowledges that privacy-related harms cannot always be measured in terms of economic or physical injury; acknowledges the lack of accountability companies and their leadership currently enjoy, seeking to hold both companies

and their executives responsible for their actions; promulgates regulations that are respectful of and acknowledge the fact that internet-age companies rely on user data in order to deliver their products and services; and requires the standardization of Application Programming Interfaces (APIs) and notices provided to consumers.[I] Currently a discussion draft and not yet introduced in Congress, this report also recommends seven key changes/additions to further enhance the Act's effectiveness:

1. Require that impact assessments of high-risk automated decision systems be made confidentially available to FTC in order to ensure that public interest harms are addressed.
2. Enable FTC to audit the annual reports companies are obligated to submit under the Act and assess whether such audits could be performed autonomously.
3. Add provisions prohibiting the reidentification of previously deidentified data and prohibiting the deidentification of data in order to circumvent having to disclose any such data to the individual to which it pertains.
4. Assess the feasibility of a data minimization provision, requiring that companies collect only the minimum data necessary to deliver to a consumer their requested product or service.
5. Add provisions ensuring that the privacy policies companies provide to consumers are clear and concise.
6. Require that companies obtain opt-in rather than opt-out consent regarding third-party information sharing and tracking.
7. Define or provide examples of the types of noneconomic impacts that constitute substantial injury under the standard of proof in the FTC Act.

With the above changes, the Consumer Data Protection Act provides common-sense protections for American consumers while respecting and acknowledging the fact that internet-age companies rely on user data in order to deliver their products and services.

[I] Application Programming Interfaces are a system of tools and resources for building software applications. APIs may include specifications regarding data structures, routines, variables, or object classes.

Problem Framing

According to former FCC chairman Tom Wheeler, "[the internet is] the most powerful and pervasive platform in the history of the planet."[3] While Americans have always valued privacy, never has it been more threatened than in the internet age. The Internet has a complicated relationship with privacy. Personal information is used to deliver new and innovative products and services to consumers, sometimes at no monetary cost. In these scenarios, consumers "pay" for services via access to their data. Advances in computing power and increasingly sophisticated algorithms and analytical techniques have led to the proliferation of companies whose business models are dependent on the acquisition of as much information as possible about the consumer.[4] While many companies responsibly manage their collection and use of this information, some act in an "irresponsible or reckless" manner.[5] The opaqueness and lack of Federal oversight regarding these companies' data practices has resulted in information asymmetries between private industry, and both consumers and the Federal Government. These asymmetries have led to an "arms race to use all means possible to entice users to give up more information, as well as to collect it passively through ever-more intrusive means-"[6] a market failure. Concurrently, problems relating to and within the Federal Trade Commission have weakened its ability to protect consumers, resulting in regulatory failure.

Scope

Though this report has applicability to all commercial entities that collect or use consumer data, it seeks to address one specific category of company- "tech giants." This report defines "tech giants" as entities who: 1) as a core business function, collect, utilize, store, disclose, or share an individual's data; 2) have +1 million customers;[II] and 3) do not pass IRS's gross revenues test.[III]

While data brokers and broadband internet access service (BIAS) providers have also categorically been identified as threats to consumer privacy, these companies are ancillary players in the digital marketing ecosystem,[IV] whereas tech giants operate their own full-service technology stacks and dominate their respective markets.[V] Tech giants have "become so large and valuable that they resist conventional instruments of oversight."[7] The size of these businesses' physical infrastructure, sheer quantity of data available to them, and technological sophistication "constitutes an unassailable market advantage that leads inexorably to natural monopoly."[8] Note that while this report does not include BIAS providers as a category, within its

[II] A million-consumer floor allows for the exemption of small businesses who collect data for methods such as maintaining consumer accounts or local marketing, examples of such businesses may be local "Mom and Pop" shops. The floor also allows for the exemption of start-ups, thereby encouraging new business growth and promoting innovation.

[III] In accordance with 26 U.S.C § 448(c), IRS considers any entity whose average annual gross receipts for the 3-taxable-year period preceding the current fiscal year exceeds $25 million as not eligible for classification as a small business. For more, see https://www.law.cornell.edu/uscode/text/26/448.

[IV] See Appendix I for an overview of data brokers and BIAS providers.

[V] According to industry publications, in 2017, the global digital advertising market grew 21% in size to $88 billion, with Facebook and Google alone accounting for 90% of growth globally, and 63.1% of all U.S. digital ad revenue. Sluis, "Digital Ad Market Soars To $88 Billion"; "The Digital Advertising Stats You Need for 2018," 49.

scope, some (e.g. Verizon) do meet the "tech giant" definitional threshold, and as such are included in scope.[VI]

Consumers and Private Industry

According to ex-Facebook executive and White House advisor Dipayan Ghosh, the problem is "in large part because [companies] operate out of sight of the consumer."[9] Information asymmetries allow companies to collect more data than consumers would prefer, or had consented to, if the asymmetry did not exist.[10] Companies have an interest in not sharing the data they possess with anyone else, including the individual who created it.[11] As such, consumers "generally lack a full understanding of the nature and extent of [a company's] data collection and use,"[12] and are therefore unable to make informed choices regarding their privacy. What privacy policies companies do provide are not designed for consumers' benefit, instead they are "written by lawyers, for lawyers, to protect the company."[13]

As a result, consumers face a "variety of [harmful] practices, including price discrimination in retail markets, quantity discrimination in insurance and credit markets, spam, increased risk of identity theft, and the disutility inherent in just not knowing who knows what or how they will use it in the future."[14] Asymmetries also mean that consumers may be fooled by the illusion of choice or outright lied to when making privacy decisions. A White House report found that a lack of transparency exposes consumers to serious public interest harms, such as reinforcing social inequalities or stigmatizing already marginalized minority consumers.[VII]

Government and Private Industry

Current Federal measures meant to protect consumers are outdated and inadequate, lagging behind the evolutionary pace of industry.[15] Sans a handful of sector-specific laws, the Federal Government has preferred self-regulation within the internet sector, believing regulation would stifle innovation.[16] Self-regulation has instead given tech giants leverage to negotiate privacy frameworks on their own terms, without needing to listen to input from government, or consumer advocacy groups.[17] For tech giants, profits trump the rights of consumers; companies have and will continue to seek out ways to circumvent laws and regulations that prioritize consumer privacy and transparency over their profit interests.[18]

While FTC's Bureau of Consumer Protection, and Division of Privacy and Identity Protection, are responsible for protecting consumer privacy and against unfair, deceptive, and fraudulent business practices, the Commission's current enforcement efforts have been criticized as "shockingly lax."[19]

[VI] This is necessary, as larger BIAS providers do operate their own full-service technology stacks. For instance, Verizon's Oath is likely the most sophisticated digital advertising stack outside of Facebook and Google. Ghosh and Scott, "Digital Deceit II," 24.

[VII] The White House was especially concerned with the use of artificial intelligence and machine learning in automated decision-making processes within companies. "Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights," 5; Ghosh and Scott, "Digital Deceit II," 19–20.

Privacy

Leading Privacy theorist Daniel J. Solove has developed a privacy taxonomy that identifies 12 privacy-related harms individuals suffer.[VIII] This taxonomy has merit, as it: 1) specifically addresses internet-age privacy issues; 2) accounts for issues that have achieved significant social recognition; and 3) uses a comprehensive array of multidisciplinary sources.

Data collection methods employed by the internet sector grow evermore invasive, eroding consumers' privacy. As a result, Americans suffer from "data insecurity," with many finding their lack of control "deeply troubling and [wanting data collection] limits put in place;" few expressed confidence that their data would remain "private and secure."[20]

Americans will continue to suffer from a lack of control over their privacy so long as market and regulatory failures exist. Privacy violations typically only come to FTC and the consumers' attention after they make national headlines. Privacy serves as "a restraint on how organizations use their power," as privacy, or lack thereof, is incorporated into a company's practices and procedures.[21] Thus far, tech giants have made their own rules, in their own best interests, at the expense of privacy.

Background

Privacy in America

Americans view privacy as a tenet of a decent and civilized society, as such, privacy infringements are considered societal violations.[22] Privacy online is especially valued, with 74% of respondents in one Pew study claiming that being in control of *who* can get information about them is "very important."[23] Regarding privacy, a majority of Americans do not trust online advertisers, social media sites, online video sites, search engine providers, companies/retailers they do business with, email providers, and phone companies. Over 50% of respondents stated that they were either "not at all confident," or "not too confident" that their data would remain private and secure with these companies.[24]

The value Americans place on privacy is especially apparent through the growing uneasiness regarding the data collection practices of private industry; Post-Cambridge Analytica, 54% of Facebook users surveyed claimed to have changed their privacy settings in the past 12 months.[25] Similarly, 86% of respondents in a separate Pew survey claimed to have taken actions to remove or mask their digital footprints (i.e. clearing cookies); 55% state that they would like to do more, but are unsure how.[26]

Privacy is most often discussed as an individual right, due to the American liberal tradition, and thus, is framed almost exclusively in individualistic, rather than societal, terms.[27] There is a rich legal history for this framing, including the Privacy Act of 1974.[28]

[VIII] See Appendix II for an overview of Solove's privacy taxonomy.

Privacy's Legal Basis

Privacy rights predate America itself, having originated in English common law. [IX] In the early 1600s common law developed "castle doctrine," asserting that an individual was not obligated to retreat from an attacker, provided they were inside their home.[29] Castle doctrine recognized an individual's home as "impregnable, often, even to officers engaged in the execution of [the common law's] commands-"[30] private. As the American legal system is derivative of English common law, privacy found its way into our own legal system.

In 1890 Samuel D. Warren and Louis D. Brandeis penned "The Right to Privacy," arguing that an individual's "private and personal affairs shall not be laid bare to the world."[31] Their work "did nothing less than add a chapter to the law," and has been cited in Supreme Court (also "USSC," the Court") decisions.[32] Warren and Brandeis similarly identify common law as the basis for privacy rights.[33] They argue that individual legal rights have broadened to include "the right to be left alone."[34] They further conclude that "property" had been reconceptualized to include both tangible and intangible possessions,[35] building on the Fourth Amendment's guarantee of security for the peoples' "persons, houses, papers, and effects."[36] Written 129 years ago, Warren and Brandeis wrote in response to privacy invasions from "recent inventions and business methods."[37] Their arguments still have purchase today, though whereas they concerned themselves with journalism and photography, today's focus is the internet sector.

While "The Right to Privacy" was co-authored by future-Justice Brandeis, it was not until 1965 that USSC recognized privacy in a majority opinion.[38] In *Griswold v. Connecticut*, the Court found that while not explicitly mentioned in the Constitution, the First, Third, Fourth, Fifth, and Ninth Amendments implied the right of privacy; Justice Harlan, in the concurring opinion, also cited the Fourteenth Amendment.[39] Two years later, in *Katz v. United States*, the Court found that the Fourth Amendment protects people rather than places, and, echoing "The Right to Privacy," governs intangible possessions.[40] Writing for the majority in *Katz*, Justice Stewart stated that the government's "eavesdropping activities violated the privacy upon which [Katz] justifiably relied," [41] subjecting him to unreasonable search and seizure- a violation of the Fourth Amendment. *Katz* is often celebrated as having saved the concept of privacy in the United States.[42]

The most relevant case for this report is *Carpenter v. United States* (2018), wherein the Court examined whether the warrantless search and seizure of cell phone records, to include the location and movement of individuals, violated the Fourth Amendment.[43] The Court ruled in favor of Carpenter, rejecting the government's argument that people essentially forfeit any right to privacy otherwise afforded when they use "popular technologies."[44] Other cases where the Court decided on privacy issues are *Eisenstadt v. Baird*, *Roe v. Wade*, and *Lawrence v. Texas*.[X]

[IX] The original conceptualization of privacy rights under the English common law system only provided remedy for physical interference with life and property, the tort for which is trespass vi et armies.
[X] Though privacy-related, these cases are not discussed further as they deal with privacy in regard to reproductive rights and sexuality, rather than in a context relevant to this report.

Public interest in privacy faded until the 1960s, when a number of "technological changes that appeared to threaten privacy"[45] brought it back into the spotlight. Chief among these changes was the advent of the mainframe computer, which enabled users to store data for longer periods of time and retrieve specific pieces of information from larger databases (e.g. sensitive information linked to a specific individual).[46] In 1956 these advances prompted the Social Science Research Council to propose the Federal Data Center, to "provide access to, and coordinate the use of, government statistical information."[47] Public outcry led to the cancellation of the 1965 proposal, as well as similar ones in 1967 and 1970.[48] Outcry was centered around what Americans had begun to suspect as far back as the 1930s- "Many agencies, public and private, were not just collecting information about them but were also capable of monitoring their habits and histories in an increasingly sophisticated fashion."[49] The Privacy Act was a response to these proposals, seeking to ensure that Federal agencies are transparent about their "personal-data record-keeping policies, practices, and systems."[50]

Legislation

The current Federal privacy framework lacks any single comprehensive policy and is instead a patchwork of industry-specific laws. Similarly, the Privacy Act only governs the data/privacy practices of Federal agencies.[XI]

Industry-Specific Laws

The healthcare and financial services industries are subject to Federal regulation; healthcare has the Health Insurance Portability and Accountability Act (HIPAA),[51] while the financial sector must abide by the Fair Credit Reporting Act (FCRA),[52] and the Gramm-Leach-Bliley Act (GLBA).[53]

HIPAA

Enacted in 1996, HIPAA is not exclusively a healthcare privacy bill, as it also a healthcare security bill.[54] Sec. 264 mandated the establishment of privacy standards for health information, resulting in a regulation dubbed the "Privacy Rule." The rule established Federal minimum standards for protecting the privacy of patients and their information and was deemed necessary as the previous patchwork of laws allowed personal healthcare information to be distributed without consent, and for no health-related reason.[55]

FCRA

Enacted in 1970 in response to public outcry over industry practices, FCRA sought to "promote accuracy, fairness, and the privacy of personal information assembled by Credit Reporting Agencies [CRAs]." It was the first Federal law addressing private industry's use of personal information, and one of the computer-age data protection laws.[56] Central to FCRA was the

[XI] See Appendix III for an outline of the provisions included in each bill.

requirement that CRAs implement "reasonable procedures" to protect the confidentiality, accuracy, and relevance of credit information."[57]

GLBA

Title V of GBLA addresses privacy concerns stemming from other parts of the bill, such as Sec. 101, repeals of the Glass-Stegall Act.[58] Public polling at the time also indicated that Americans were unhappy with the financial services industry's disregard for consumer privacy, a concern substantiated through a number of high-profile cases where banks sold consumers' information to other parties with adverse effects.[59] GLBA has received criticism for "unfairly [burdening] the individual to protect privacy with an opt-out standard;" allowing companies to use "convoluted, confusing, and misleading" opt-out policies; providing no opt-out for information sharing among industry affiliates; and having weak enforcement and compensation mechanisms.[60]

The Privacy Act of 1974

The Privacy Act was in response to: 1) public outcry regarding proposals for the establishment of a Federal Data Center;[61] 2) computing advances (e.g. mainframe computers);[62] and 3) the illegal surveillance and investigation of citizens uncovered by Watergate.[63] While the bill initially sought to include the private sector,[64] intensive industry lobbying efforts prevented this.[65]

Passed in "great haste during the final week of the [93rd] Congress,"[66] the Act is an omnibus "code of fair information practices" intended to balance the Federal Government's need for record keeping with the rights of citizens to be protected against unwarranted privacy invasions via "Federal agencies' collection, maintenance, use, and disclosure of personal information about them."[67]

Additionally, the Act established a Privacy Protection Study Commission (PPSC), tasked with studying government and private data systems and making recommendations for protecting privacy through the Act itself or additional legislation.[68] In their final report, the PPSC found that much of the language in the Privacy Act was unclear.[69] DOJ similarly concluded that the Act was difficult to apply, due to its "imprecise language, limited legislative history, and somewhat outdated regulatory guidelines."[70]

Privacy Act Amendments

In 1988 Congress passed the Computer Matching and Privacy Protection Act[71] to "ensure privacy, integrity, and verification of data disclosed for computer matching, [and] to establish Data Integrity Boards within Federal agencies,"[72] via amendment to the Privacy Act. The 1988 amendments sought to restrict data/information sharing between agencies. Congress then passed the Computer Matching and Privacy Protection Amendments, in order to clarify the due process provisions in subsection (p) of 5 U.S.C. § 522a (created by the 1988 bill). The 1990 amendments constituted Sec. 7201 of the Omnibus Budget Reconciliation Act.[73]

The Data Integrity Boards created by the 1988 Act are required in every agency participating in matching programs (data sharing arrangements with other agencies).[74] Boards are tasked with reviewing and approving all data matching agreements within their respective agencies in order to ensure compliance with all laws and guidelines and are comprised of senior agency officials. These reviews are conducted annually, submitted to the Office of Management and Budget, and must be made available to the public. The boards serve as clearinghouses for the "accuracy, completeness, and reliability of records."[75]

A History of Bad Behavior

Lobbying for exclusion from the Privacy Act, private sector argued that there was "little concrete evidence of abuses in private sector personal information practices,"[76] and thus, no legitimate basis for their inclusion. Industry also argued that they were already overburdened by government regulation, advocating instead for self-regulation in the form of voluntary protections for personal information.[77] Though successful in seeking exemption, these arguments are unequivocally false today; there is an abundance of modern-day evidence to suggest that the private sector routinely and intentionally abuses consumers' privacy. The Federal Government's inability to audit the data practices of companies results in informational asymmetries, as lawmakers and the public alike must rely almost exclusively on breaking news stories to learn of new privacy violations.

Below is an overview of privacy wrongdoings committed by the two largest players in the internet sector: Google and Facebook. While by no means the only firms committing privacy violations, their dominance within the digital advertising market,[78] and status as the 1st (Google) and 3rd (Facebook) most visited websites on earth make them useful for highlighting problems within the sector as a whole. [79] The 2nd most visited platform, YouTube, is a Google subsidiary.

Facebook

A 2019 report published by the House of Commons Digital, Culture, Media and Sport Committee referred to tech companies, explicitly naming Facebook, as "digital gangsters" who consider themselves to be "ahead of and beyond the law."[80] The report stated that Facebook's management structure "seemed to be designed to conceal knowledge of and responsibility for specific decisions," and that the company deliberately sent witnesses to Parliament who would be unable to fully answer questions they were asked.[81]

Cambridge Analytica

New York Times[82] and *Guardian*[83] first reported in March 2018 that UK-based voter profiling firm Cambridge Analytica obtained, without permission, private information from +50 million Facebook profiles worldwide. Ultimately, it was discovered that 87 million accounts were compromised.[84] Collaborating with Cambridge Analytica, the application "thisisyourdigitallife" paid Facebook users to take a personality test and consent to their data being used for "academic purposes."[85] In consenting, individuals unknowingly also gave the app access to the personal

information of their Facebook friends' profiles; only the 270,000 individuals who participated in the survey ever actually consented to having their data harvested.[XII]

While it was Cambridge Analytica who harvested data illegally, Facebook neglected its legal obligation to inform regulators and individuals about the breach.[86] Filing a lawsuit against Facebook, Washington DC district attorney Karl Racine stated, "Facebook failed to protect the privacy of its users and deceived them about who had access to their data and how it was used," and further "put [its] users at risk of manipulation" by allowing third-party applications to collect data without user consent.[87] Evidence also suggests that Facebook was likely aware of the breach months before it made headlines and "consistently mislead" UK's Parliament "about what it knew and when."[88]

Tech Giants and Special Access

Facebook has routinely disregarded its own privacy protections and regulations in order to give "some of the world's largest technology companies more intrusive access to users' personal data than it disclosed."[89] Facebook had such arrangements with +150 companies,[90] +60 of whom are device manufactures.[91] The same day *NYT* broke the story, Facebook published a statement,[92] which a former Facebook operations manager criticized as being "hugely misleading."[93] Six years before making national headlines Facebook internally flagged these arrangements as privacy issues-[94] they continued nonetheless.

While Facebook claimed that by 2019 outside companies would have less access to its data, officials hid the fact that device manufacturers would be exempted from these new restrictions.[95] *NYT* debunked Facebook VP Ime Archibong's claim that device partners could only use Facebook data to "provide versions of 'the Facebook experience,'" finding that partners could obtain a user's Facebook friends' data, even if that friend previously denied Facebook permission to share their information with third parties.[96] Exemplifying how tech giants deliberately circumvent laws and regulations, Facebook claimed that these device manufacturers were "extensions of Facebook," rather than third parties.[97] This argument was similarly employed against criticism that these partnerships violated a 2011 FTC consent order barring the company from overriding users' privacy settings without first obtaining explicit consent;[98] even if individuals had opted out of giving outside parties access their data, some device manufacturers had the ability to override that restriction.[99]

[XII] Ultimately, the data collected on those affected was comprehensive enough for Cambridge Analytica to create psychographic profiles, which they were then able to sell to interested parties. Rosenberg, Confessore, and Cadwalladr, "Consultants Exploited Facebook."

Bing	Access to friends lists of "virtually all" Facebook users, without consent
NETFLIX Spotify	Granted the ability to read Facebook users' private messages
amazon	Able to obtain users' names and contact information though their Facebook friends
YAHOO!	Access to Facebook posts of friends
	Hid indicators from users that Apple devices were asking for Facebook data

Table 1 Selected History of Special Arrangements[100]

Because of these arrangements, Facebook's advertising revenue soared,[101] again suggesting that companies prioritize profits over privacy.[XIII] These arrangements contradict, and continued after, Zuckerberg's 2018 testimony to Congress, wherein Zuckerberg stated that users have "complete control" over their data,[XIV] leading Rep. Cicilline (D-RI) to conclude that Zuckerberg likely lied to Congress.[102] Zuckerberg also told Congress that when an individual uses their Facebook account to sign into another application they do not bring information from their Facebook friends-[XV] this too has been called a lie.[XVI]

Flo Health

First reported by *Wall Street Journal*, many mobile applications send data to Facebook without "any prominent or specific disclosure,"[103] and regardless of whether the app user has a Facebook account or uses a Facebook account to sign in. Responding to *WSJ*, Facebook stated that some of the data sharing did "violate its business terms" and that it has since told applications to stop sending sensitive information.[104] An Associated Press report found that while Facebook was correct in stating that this data sharing violated its business terms, before the *WSJ* article, it accepted the data in question without protest.[105]

Facebook collected this information thought its analytic tool, App Events, which "allows app developers to record user activity and report it back to Facebook."[106] The most egregious violator

[XIII] It should also be noted that the table also provides examples of how Bing, Netflix, Spotify, Amazon, Yahoo!, and Apple, all tech giants themselves, also violate the privacy of consumers. Facebook has also cited similar arrangements used by Google and Twitter as proof that this is an industry-wide practice. Cuthbertson, "Mark Zuckerberg Lied to Congress about Facebook Data Scandal, Congressman Claims."

[XIV] See Appendix IV for the exchange.

[XV] See Appendix V for the exchange.

[XVI] In two separate tweets, Parakilas called the Zuckerberg's claims "not correct," and "not a small misstatement." *See*: Sandy Parakila, Twitter post, June 4, 2018, 12:44 am; Sandy Parakila, Twitter post, June 4, 2018, 12:44 am.

uncovered by *WSJ* was Flo Health Inc.'s Period and Ovulation Tracker, and app with +25 million active users, which sent Facebook information about when a user was having her period, or whether she informed Flo that she was attempting to get pregnant.[107] Flo claimed that any data sent to Facebook was "depersonalized," but testing found that data could easily be connected back to a specific individual.[108] NY Governor Cuomo called the arrangement a "clear [invasion] of consumer privacy."[109]

Facebook claims that "some" of the sensitive information third parties send is automatically deleted, but this was likely not the case for Flo Health.[110] For Facebook to automatically delete sensitive data sent by Flo, it would needed to have previously been identified as sensitive by Facebook, but this should have prompted them to instruct Flo to stop sending it, long before the story went public.

While Facebook (allegedly) allows users to opt out of allowing the company to use third-party data for targeted advertising,[111] this is of no help to users of third-party applications who do not have Facebook accounts. Facebook CFO David Wehner told investors that having to tighten privacy controls for apps such as Flo Health is an "ongoing risk that we're monitoring,"[112] again exemplifying how companies prioritize profit over privacy. This statement also suggests that Facebook was in fact interested in the data Flo sent, as identifying its loss as a risk to profits implies that it has value.

Facebook Messenger

In 2018 a Federal lawsuit was filed against Facebook for its harvesting of phone and texting data from Android-based phones.[113] According to the suit, individuals who accessed Facebook Messenger or Facebook Lite on Android devices unknowingly gave Facebook access to their call and text records when opting in to importing their phone contacts to the application.[114] Facebook's response[115] to the lawsuit was characterized as "the first time [Facebook] actually spelled out [the practice] in clear terms for users-"[116] a separate investigation found even the response itself to be misleading.[117]

It was also discovered that Facebook Messenger used popup notifications to trick users into giving the app access the address book of iOS-based devices.[118] Instead of explicitly asking users for permission to access their address books, the permission claimed it would allow users to "text anyone in [their] phone." Users could either select "OK," or "Learn More;" the "OK" option had a blinking arrow pointing to it. Clicking on "Learn More" provided the user with a large blue button labeled "Turn On" and a much smaller "Not Now" option. The "Lean More" page's claim that skipping the import process means "[users] will need to add each contact one-by-one to message them" is false, as contacts who are Facebook friends already automatically populate on the Messenger friends list.

Google

Nest

In 2014 Google purchased Nest Labs, a smart home device manufacturer, for $3.2 billion.[119] In February 2019 Google announced that a software update to Nest's home security system would make Nest Guard, the system's keypad and alarm module, compatible with Google Assistant.[120] Business Insider found one major problem with the update- in no product material was it ever disclosed that Nest Guard contained a microphone.[121]Google responded, claiming that the nondisclosure was an error and that they never intended for the microphone to be a secret.[122] Many were unconvinced by Google's response, with NYU Stern professor Scott Galloway tweeting: "Oops! We neglected to mention we're recording everything you do while fronting as a security device. The fact that we can record you is in no way intentional, a mic must have fallen into the device."[123] The Electronic Privacy Information Center (EPIC) concurred, calling the move "criminal,"[124] and their director of cyber security tweeting that it was "deliberately misleading."[125]

The privacy statement for Nest Cam,[126] a series of home cameras, is similarly misleading, stating, "Nest Cam enables *you* to determine the purpose and means for which you collect video and audio signals data;" the statement *does not* say the user has control over how/why *Nest* collects that data. Nowhere does Nest inform the consumer that video and audio signals may be used to surveil a user's home in order to lean of a user's preferences for future targeted advertising, a function for which Google has filed a patent.[127]

The Safari Workaround

The Apple iPhone's default browser is Safari, whose default privacy settings block all third-party cookies. From June 1, 2011, to February 15, 2012, Google intentionally circumvented Safari's default security settings on the devices of an estimated 5.4 million individuals.[128] To do this, Google created the "Safari Workaround," which consisted of placing a piece of JavaScript code on iPhones that was able to bypass Safari's default settings in order to place a Google tracking cookie on the device.[129] Previously, Google had publicly assured that it would never do such a thing.[130] In 2012 Google was fined $22.5 million by FTC for again misrepresenting that "it would not place tracking 'cookies' or serve targeted ads to [Safari] users," and for circumventing Safari's default private settings.[131] Google has twice been charged for the same offense, displaying an intentional effort to lie to and deceive consumers.

The Illusion of Choice

While Google claims to offer users the ability to "turn off" location services, the process is difficult, with researcher and professor Zeynep Tufecki stating, "it took me three tries to completely turn off Google location tracking. I kept thinking I had turned it completely off, and it would just pop back up. If I can't manage this, who is supposed to? I have a technical background and write/research about all this for a living."[132] It was also discovered that phones

running the Google-developed mobile operating system, Android, gather and send location data to Google regardless of whether the phone's location services option has been "turned off."[133] Similarly, Google is currently being sued over claims that it tracks the location of both Android and iOS devices, even when "location history" is turned off- computer science researchers at Princeton University have confirmed these allegations.[134]

Google's "Ad Personalization" webpage contains a list of "Topics You Like" based on an individual's activity on Google services (e.g. Gmail or YouTube) and +2 million "partner websites."[135] These topics are used to generate personalized ads.[136] The page provides individuals with the option of deleting topics from the "Topics You Like" category, but this only places them into the "Topics You Don't Like" category, essentially tricking users into giving Google further insight into their personal preferences. Near the top of the page is an obscure slide-lock icon, void of any labeling, which only upon clicking reveals that it turns off ad personalization. This is a rather pointless option, as it appears turning off ad personalization only means that consumers no longer see targeted ads, rather than actually disabling any ad personalization-related data collection.

The Federal Trade Commission

In 1914 FTC was established by the Federal Trade Commission Act, in order to "[prevent] unfair methods of competition in commerce."[137] The Commission was a major tool for President Wilson in the battle against monopolies. The Bureau of Consumer Protection is responsible for overseeing investigations pertaining to internet privacy through its Division of Privacy and Identity Protection. As such, FTC is the lead agency for internet privacy matters. Statutory authority rests in Section 5(a) of the FTC Act, whose 1938 amendment further prohibited unfair and deceptive business practices.[138]

For FTC to take action under Section 5, it must first identify an act as unfair or deceptive. FTC defines "unfair" as an act or practice that "causes, or is likely to cause, substantial injury not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition as a result of the practice."[139] The "substantial injury" requirement is problematic, as privacy harms can be "repeated, untraceable injuries far removed in [time and place] from that practice that caused the harm,"[140] especially in the internet age. Previously, FTC has used "unfairness" against companies who failed to protect consumer data.[141] "Deceptive" is defined as "a representation or omission, if it is material and likely to mislead consumers acting reasonably under the circumstances."[142] While a company violating its own privacy policy is considered deceptive, the definition has a major flaw; as long as companies do not explicitly bar themselves from certain activities in their privacy policies, those actions cannot be considered deceptive.

For the Commission to begin investigating a consumer privacy issue, it must first receive a formal complaint. Complaints originate from within industry, consumers, other Federal and non-Federal agencies, Congress, and internally.[143] In requiring a formal complaint to initiate an investigation, FTC is greatly constrained in protecting consumer privacy, and is unable to proactively protect consumers. Informational asymmetries compound this problem, as having reason to believe that an entity has committed an unfair or deceptive practice requires knowledge of such a practice occurring. While only a selected history of misconduct by tech giants, "A

History of Bad Behavior" demonstrates unequivocally that companies cannot be trusted to self-regulate, nor can it be expected that they will follow rules put in place by themselves or others.

Historically, when FTC receives a complaint and decides that a violation has taken place, it has entered into a settlement agreement, known as a consent order, with the offender, requiring them to take action to remedy the issue. The below chart outlines these actions and their problems:

Action:	Problem:
Implementing reasonable privacy/security programs	Discussed in "Tech Giants and Special Access," companies actively seek out ways to circumvent their own privacy policies/programs.
Subjecting to long-term monitoring of compliance with consent orders by outside entities	Audits are not government-led. PricewaterhouseCoopers reported favorably on Facebook, failing to catch Cambridge Analytica in its audit, exemplifying how third-party audits are not by default more reliable than those conducted by companies themselves.[144]
Monetary redress to consumers	Privacy injuries are difficult to quantify, and usually only substantial in the aggregate.[145]
Disgorgement of ill-gotten gains	Not punitive- does not serve as deterrent to others. Difficult to quantify monetary value of individual data streams.
Deleting illegally-obtained information	Information may have already been sold or shared to a third-party. Data's value may have already been extracted by the time a consent order comes into force.
Providing transparency and choice mechanisms	Discussed in "The Illusion of Choice," companies may completely disregard consumer choices, or make choice mechanisms intentionally difficult to operate. Privacy policies not designed for consumers-[146] they are lengthy and "on average, require two years college education to comprehend."[147]

Table 2 Issues with Consent Orders

Of the 101 privacy-related enforcement actions filed by FTC since 2009, almost all have resulted in consent orders; in two cases FTC sought civil penalties as well.[148] Civil penalties are only available after a company violates a final consent order, harming consumers as companies get "a first free pass and must be found to neglect reasonable practices twice before they face a substantial penalty."[149] Generally, tech giants consider fines just the cost of doing business.

Despite being the lead agency for the issue, FTC has thus far not promulgated regulations regarding internet privacy. FCRA, GLBA, and HIPAA all provide precedence for a Federal organization to regulate privacy issues within the private sector, while the Privacy Act and its amendments are excellent examples of government-mandated boards responsible for overseeing privacy issues. Hindering FTC's ability to impose such regulations is Title I of the FTC Improvements Act, the Magnuson-Moss Warranty,[150] which was in response to concerns of FTC regulatory overreach in the 1970s. Magnuson-Moss requires that before FTC issues notice of a proposed rule, it must publish an advance notice in the *Federal Resister,* invite comments and alternative suggestions, submit the advance notice to relevant Senate and House committees, and determine that unfair or receptive acts have taken place.[151] FTC staff have identified Magnuson-Moss as adding "significant procedural limitations and requirements" to the rulemaking process;[152] under Magnuson-Moss, it takes on average 5.26 years to make a rule, but when directed to use the Administrative Procedures Act (APA), FTC was able to issue "dozens of" rules in only 287.25 days.[153]

According to the 2018 Agency Financial Report, FTC has 1,114 full-time employees, and a $306 million budget.[154] While FTC has had a number of modest privacy victories in the past, Ghosh concludes that FTC's overall privacy enforcement is "shockingly lax," due to staffing and budget shortages.[155] The outsourcing of consent order compliance auditing to firms such as PricewaterhouseCoopers is suggestive of Ghosh's criticism; given its size, FTC would unlikely be able to effectively audit tech giants while simultaneously continuing with other privacy-related activities. Currently, FTC relies on about 50 staff members to police the entire technology sector- these same individuals are also responsible for policing credit agencies.[156] Federal privacy legislation that fails to account for FTC's internal problems will only exacerbate them. The success of any Federal privacy regime rests on the Commission's ability to effectively carry out its mandate.

Evaluative Criteria

This report has thus far explained how market and regulatory failures have allowed for tech giants to exploit American consumers and their privacy. As such, any Federal privacy framework must simultaneously address: 1) informational asymmetries between tech giants, and both the USG and consumers, which has resulted in market failure; and 2) FTC-specific problems resulting in regulatory failure.

1. Market Failure:
    a. Reduce informational asymmetries through an auditing/reporting mechanism with Federal oversight.
    b. Improve transparency for consumers regarding tech giants' data practices.
2. Regulatory Failure:
    a. Promulgate baseline data/information principles.
    b. Grant FTC enhanced rulemaking privileges.
    c. Allow FTC to assess civil penalties for first-time violators.
    d. Address FTC's staffing and funding issues.

These criteria serve as a baseline for evaluating the potential effectiveness of any legislation seeking to establish a Federal privacy framework and have been developed based on the case studies provided in this report's background section, and recommendations from FTC, privacy experts, and White House staff.[157]

Considered Alternatives

In recent years there have been numerous privacy framework proposals- this report analyzes only current legislative proposals from members of Congress. This is a favorable methodology as the preponderance of policy papers offer only broad and imprecise recommendations, such as "companies should offer simplified consumer choice,"[158] "ensure robust enforcement,"[159] or "establish clear consumer rights."[160] As can be seen in the reports cited in endnotes 158-160, most proposals make some variation of the same recommendations- analyzing these proposals would be analogous to analyzing the same proposal written three different ways. Contrastingly, the following bills provide explicit provisions operationalizing their respective privacy frameworks, providing policy alternatives that can be assessed at the operational, rather than conceptual, level. There are four alternatives:

1. S.3744- Data Care Act.[161]
2. S.2639- Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act.[162]
3. S.142- American Data Dissemination (ADD) Act.[163]
4. OLL19313- Privacy Bill of Rights Act.[164]

Data Care Act

In 2018 the Data Care Act was introduced by a group of 15 Democratic senators led by Sen. Schatz (HI), who stated that online companies should legally be required to "protect and responsibly use [personal data]" in a manner similar to the healthcare and financial services industries.[165] Other senators framed the bill similarly, citing recent data breaches, revelations about the practices of the internet sector, and the huge profits companies make exploiting consumer data, as evidence that the Federal Government must step in to protect consumers.[166]

The bill establishes three duties companies must adhere to:

1. Care- reasonably secure individual identifying data from unauthorized access and promptly inform users of data breaches.[167]
2. Loyalty- cannot use identifying data, or derivatives of it, in a manner that harms consumers.[168]
3. Confidentiality – may not sell or share individual identifying data with another entity, unless said entity similarly abides by the duties of care and loyalty.[169]

"Individual identifying data" is defined as any data collected over the internet or any other digital network, that is linked, or reasonably linkable to, a specific user or device.[170]

Establish auditing/reporting mechanism with Federal oversight	**No**	N/A
Improve transparency for consumers	**Very Low**	Failure to promptly notify consumers of data breaches is designated an unfair and deceptive practice.[171] While bill would establish the first non-industry-specific Federal notification of breach requirement, all 50 States, the District of Colombia, Guam, Puerto Rico, and the U.S. Virgin Islands already have some version of beach notification legislation.[172]
Promulgate baseline data/information principles	**No**	N/A
Enhance FTC rulemaking	**Yes**	Provides for APA rulemaking.[XVII]
Allow for civil penalties	**Yes**	The attorney general of a State may seek civil penalties for violations of the Act equal to the amount calculated by multiplying an amount not to exceed $10,000, by the greater of: 1) the number of days a company was in violation of the Act, or 2) the number of users the violation harmed.[XVIII] The Act does not set a maximum limit for the size of civil penalties.
Address FTC staffing and funding	**No**	N/A

Table 3 Data Care Act Evaluation

Civil penalty provisions of the Act are strong, with the exclusion of a maximum penalty sum serving as a better deterrent than monetary redress or the disgorgement of ill-gotten gains currently do. As a privacy-related harm typically affects hundreds of thousands of consumers, rather than a single individual, the Act's formula for calculating civil penalties ensures that companies are incentivized to adhere to its provisions, deterring non-compliance while serving as a sufficiently punitive punishment for violators. The provision for APA rulemaking is similarly positive.

[XVII] APA rulemaking relieves FTC of Magnuson-Moss requirements. See Sec. 4(3) in Schatz, Data Care Act of 2018.

[XVIII] Sec.4 (b) in Schatz. The $10,000 figure is from 15 U.S.C. § 45(m)(1)(A), which states that civil penalties may not exceed $10,000 per violation. For more, see https://www.law.cornell.edu/uscode/text/15/45.

Strengths aside, failure to establish a Federally-overseen auditing/reporting mechanism, promulgate baseline data collection principles, address issues within FTC, and the presence of additional issues makes the Data Care Act an unviable recommendation.

The Act does not establish baseline data collection principles that companies would be required to follow, failing to protect individuals in the same way that, for example, HIPAA does. HIPAA establishes concrete and explicit regulations that its covered entities must follow, while the Data Care Act promotes the overly simplified duties of Care, Loyalty, and Confidentiality. What expanded rulemaking privileges are provided are of little benefit, as the Commission is limited to promulgating regulations regarding exemptions from the bill,[173] enforcement of the duties,[174] and breach notification requirements.[175] FTC cannot promulgate further privacy-enhancing regulations.

The only reporting/auditing mechanisms present are: 1) the obligation to inform consumers of unauthorized breaches; and 2) requiring that companies audit third parties granted access to consumer data.[XIX] Neither mechanism reduces informational asymmetries for consumers or the government, forcing parties to blindly trust that companies are self-regulating. This report's background section has shown: 1) that Facebook has previously deliberately hid data breaches from the public, likely lying to Parliament about it; and 2) tech giants refuse to self-regulate.

The Act's scope covers any entity engaged in interstate commerce via the internet, or any other digital network, that collects individual identifying data about its users.[176] This fails to differentiate between tech giants and small businesses/start-ups. According to the U.S. Chamber of Commerce Foundation, Federal regulations disproportionately affect small business, costing those with less than 50 employees 20% more than the average for all firms-[177] the average startup has ~5 employees.[178] Scope is also detrimental as FTC is not provided additional resources to enforce the Act; the already understaffed, underfunded, Privacy Division would be responsible for enforcing a regulatory framework encompassing potentially tens of thousands of businesses.[XX]

A number of issues undermine the duties of Care, Loyalty, and Confidentiality. The inclusion of "unauthorized access" in the Duty of Care is troublesome,[179] as the bill fails to specify what constitutes unauthorized access. Discussed in the background section, Facebook circumvented its own privacy policy by claiming that companies with whom it held special arrangements were "extensions of Facebook," rather than third parties.

The Duty of Loyalty fails to regulate actual data collection, instead only governing how companies use data post-collection, making consumers susceptible to privacy-related harms

[XIX] Sec. 2 (b)(1)(B) and Sec. 2 (b)(3)(C) in Schatz, Data Care Act of 2018. , respectively. Compliance audits are to be carried out by the company that provided the third party with access to their consumers' information.
[XX] According to the Small Business Administration, there are 30.2 million small businesses in the U.S. as of 2018, as scope applies to any and all businesses that collect individual identifying data, any small business that collects information from customers over the internet is potentially affected by the Act. U.S. Small Business Administration, "2018 Small Business Profile."

during collection.[XXI] Loyalty also fails to acknowledge that privacy-related harms are not always physical or financial, and are instead often untraceable, and far removed in time and place from the practice that caused the harm.[180] As FTC would need to prove that a certain practice would likely result in material physical or financial harm, [181] enforcement action on grounds that, intrinsically, a specific data collection practice is harmful is precluded. The Duty does prohibit using data in a manner that would be "unexpected and offensive to a reasonable end user,"[182] but does not define "unexpected," "offensive," or "reasonable end user."

The Duty of Confidentiality does not require that companies receive explicit consent from consumers before sharing or selling their data to third parties, instead requiring only that these practices are consistent with the duties of Care and Loyalty- consumers have no agency over what companies collect or how they use it. If tech giants are able to find ways to work around the duties of Care and Loyalty, they will have freed themselves from any obligation otherwise imposed under the Duty of Confidentiality; comments from the head of DOJ's Antitrust Division, and Harvard Law professor Susan Crawford indicate that this is highly probable.[XXII]

Finally, while civil penalty provisions are provided, they are only available as a first-time remedy for State attorney generals. The Act would require that FTC still rely on consent orders as its primary enforcement mechanism.

CONSENT Act

In 2018 Sen. Markey (D-MA) and Sen. Blumenthal (D-CT) introduced the CONSENT Act, claiming, "America deserves a privacy bill of rights that puts consumers, not corporations in control of their personal, sensitive information," and that "the startling consumer abuses by [tech giants] necessitate swift legislative action rather than overdue apologies and hand-wringing."[183]

Sen. Markey's website claims the bill has four major provisions,[184] requiring that edge providers:

1. Obtain opt-in consent from consumers to use/share/sell their personal information;[185]
2. develop reasonable data security practices;[186]
3. notify consumers about how their information is collected, used, and shared;[187] and
4. notify consumers of data breaches.[188]

"Edge providers" are defined as any entity that provides a service over the internet that: 1) requires customers to subscribe or establish an account; 2) customers purchase from the provider without subscription or account; 3) is a search engine; or 4) through which a customer divulges sensitive or personally identifiable information.[189]

[XXI] As a point of clarification, the duty of confidentiality does address privacy, however only in the context of sharing consumer information with third parties. See Sec. 2(3) in Schatz, Data Care Act of 2018.
[XXII] "I want to actually at this point align myself with the head of the Antitrust Division at the Department of Justice, right now, who has said that clever lawyers can work around any set of rules you put in place in words." Harvard Institute of Politics, *Big Tech and Democracy*.

Establish auditing/reporting mechanism with Federal oversight	**No**	N/A
Improve transparency for consumers	**Moderate improvement**	Requires that companies: notify consumers about the collection, use, and sharing, of their information; update consumers when privacy/data policies are significantly changed; and notify consumers of security breaches.[190]
Promulgate baseline data/information principles	**Yes**	Instructs FTC to promulgate regulations to protect consumer privacy within one year of the Act's enactment and to ensure that said regulations take effect within 180 days.[191]
Enhance FTC rulemaking	**Yes**	Provides for APA rulemaking.[192]
Allow for civil penalties	**Yes**	The attorney general of a State may seek civil penalties.[XXIII]
Address FTC staffing and funding	**No provision-exacerbates current problems**	Fails to address FTC issues, and under certain circumstances requires other unequipped agencies to enforce the Act.[193]

Table 4 CONSENT Act Evaluation

CONSENT's strengths include the prohibition of take-it-or-leave-it service offers in order to gain access to customer data;[194] establishing baseline regulations companies must follow;[195] requiring opt-in, rather than opt-out consent;[196] and requiring consent before using, sharing, or selling sensitive consumer information.[197] Banning take-it-or-leave-it offers is particularly noteworthy, as it protects consumers from coercion, while also acknowledging that consumers cannot just "leave-it," given the integral role the internet plays in modern America.[XXIV] Similarly, requiring

[XXIII] The Act's actual text provides a State's attorney general with the ability to take civil action to enjoin an action in violation of the bill; enforce compliance with the bill or appropriate regulation; obtain damages, restitution, or compensation for residents of the state; or obtain other relief considered appropriate by the court. This text provides for the authority to seek civil penalties. See Under Sec. 2(e)(1)(A) Markey, CONSENT Act.

[XXIV] For example, many Americans claim social media affords them important and meaningful social interactions such as staying in touch with far-flung friends and family. Social media also provides for civic and political participation and the dispersion of news. Rainie, "How Americans Feel about Social Media and Privacy."

that companies obtain opt-in rather than opt-out consent before using/sharing/selling consumer information addresses the criticism that opt-out mechanisms harm consumers.[xxv]

The lack of any auditing/reporting mechanism, and failure to address FTC's issues while simultaneously requiring "certain other agencies" to enforce the Act make it an unfavorable recommendation.

Similar to the Data Care Act, CONSENT's scope is problematic, as it does not differentiate between tech giants and small businesses/start-ups. Scope is predicated entirely on whether a company's business model possess certain characteristics, rather than whether a company collects/uses/stores/shares an individual's data. This is an issue as it excludes large BIAS providers. While Sec. 2(f) does provide for the inclusion of telecommunications carriers, the term "but only to the extent that the telecommunications carrier is operating as an edge provider" still excludes BIAS providers, due to the edge provider definition. Comments from the broadband industry's principle trade association suggest BIAS providers have a vested interest in the Act's passing.[xxvi]

Agencies identified as responsible for enforcing the Act is another issue. Aside from FTC, Sec. 2(d) designates the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve, the National Credit Union Administration Board, the Secretary of Transportation, the Secretary of Agriculture, and the Farm Credit Administration, as responsible for CONSENT's enforcement. It is unrealistic to expect that these organizations, which do not specialize in consumers' rights or data/ privacy issues, have the capacity to enforce CONSENT. The Act provides no appropriations for its enforcement for FTC or the seven others.

The Act does not establish any auditing/reporting mechanism, Federally-overseen or otherwise. While it does provide for APA rulemaking in order to promulgate baseline privacy regulations and improve transparency for consumers, FTC and consumers alike are provided no means to ensure that regulations are followed, and that transparency is actually improved.

Finally, while the Act does provide for civil penalties, the exclusion of guidance regarding the size of damages is of advantage to companies, given the recent events regarding punitive damages in the American legal system. Though USSC has refused to provide concrete constitutional limits on punitive damages, guidance it has put out suggests that no more than a single-digit ratio between punitive and compensatory damages is permissible.[198] In April 2018 the Tenth Circuit reduced punitive damages from a ratio of 11.5:1 to 1:1 in a carbon monoxide poisoning case, citing the due process provisions of the 14th Amendment.[199] Damages of this size are hardly punitive for tech giants, who already see multi-billion-dollar fines as just the cost of doing business. FTC may intervene in a civil action brought by a State's attorney general, but does not itself have the ability to seek civil penalties, requiring instead that it continue to rely on

[xxv] This issue was first raised in regards to the opt-out provision of the Gramm-Leach-Bliley Act. Electronic Privacy Information Center, "The Gramm-Leach-Bliley Act."

[xxvi] The Internet & Television Association claims BIAS providers (ISPs) are unfairly criticized for own data practices, passing the buck to edge providers. Eggerton, "NCTA's Powell: Net Neutrality Debate Is Increasingly Irrelevant."

consent orders as its primary enforcement mechanism. The additional agencies have no right to intervention; should companies under their purview be subject to civil action, they cannot petition for appeal, or be heard with respect to any matter that arises in the action.

ADD Act

In January 2019 Sen. Rubio (R-FL) introduced the American Data Dissemination Act, stating that while there was growing consensus that Congress needed to take action to protect consumer privacy, "any efforts to address [privacy] must also balance the need to protect the innovative capabilities of the digital economy that have enabled new entrants and small businesses to succeed in the marketplace."[200] The bill borrows heavily from the Privacy Act, and claims three major provisions:

1. No later than 180 days after ADD's enactment, FTC must submit detailed privacy recommendations, modeled on the Privacy Act, to Congress.[201]
2. Within one year of submitting its recommendations, FTC must publish and submit to Congress proposed regulations, modeled on the Privacy Act, which would impose privacy requirements on the applicable companies.[202]
3. If Congress does not enact a law based on FTC's recommendations within two years, FTC has three months to promulgate regulations imposing privacy requirements.[203]

Establish auditing/reporting mechanism with Federal oversight	**No**	N/A
Improve transparency for consumers	**Very low**	Only explicitly requires that companies, upon request, provide a consumer with access to records held on them, however, companies have the option of deleting the relevant records instead. Also requires that companies keep an accounting of certain disclosures of records, which upon request must be made available to consumers, but there are potential loopholes.[204]
Promulgate baseline data/information principles	**Yes**	Sec. 4 technically requires FTC to promulgate regulations pertaining to disclosure, transparency, accuracy, fair information practice principles, and recordkeeping, however Congress would need to pass additional legislation to enact them.
Enhance FTC rulemaking	**No**	N/A
Allow for civil penalties	**No**	N/A

Address FTC staffing and funding	**No**	N/A

Table 5 ADD Act Evaluation

ADD's single strength is its concern for small businesses and startups. While the bill defines its scope as any company that provides a service that uses the internet and collects records,[205] Sec. 4(b)(1)(A) provides for the establishment of criteria for "exempting small, newly formed covered providers."[XXVII] ADD is the weakest of the alternatives analyzed, as it does not address the need for an auditing/reporting mechanism, FTC rulemaking, civil penalties, or FTC staffing and funding. While Sec.4 does address transparency and baseline regulations, it does so indirectly and with limited scope.

Aside from failing to address four of the evaluative criteria, the three provisions outlined by Sen. Rubio are ADD's biggest deficiency. The Act itself does nothing to protect consumers, especially in the near future; instead of promulgating regulations, ADD instructs FTC to make, separately, privacy and regulatory recommendations to Congress, who must then pass an entirely separate law enacting them. This scheme is especially troublesome as Congress lacks a sophisticated understanding of how the internet works.[XXVIII] There is no logical reason why FTC, with its expertise, should not be trusted to promulgate regulations itself. If Congress fails to enact a law imposing FTC's recommendations, FTC must then promulgate final regulations within three months. As such, FTC must use Magnuson-Moss Warranty rules. Reliance on the Warranty raises concerns as to whether the three-month timeframe provides sufficient time to promulgate regulations, and to what degree FTC's initial regulatory recommendations must undergo revision due to under Magnuson-Moss.[XXIX] That ADD sets a deadline of 27 months after its enactment for final regulations to come into effect means tech giants may be completely free of any regulatory oversight for 27 months, plus however long it takes Congress to pass ADD.

The Act's reliance on the Privacy Act is problematic, as the Privacy Act has previously been criticized as being outdated and using imprecise language by DOJ and PPSC.[206] Throughout, ADD defers to the text and provisions of the Privacy Act rather than developing its own concepts and guidelines. In accordance with the Privacy Act, ADD relies on self-regulation.[XXX] Questions pertaining to the bill's reliance on the Privacy Act also arise when discussing transparency, particularly in Sec.4 (b)(G), which requires that companies keep an accounting of certain

[XXVII] That the FTC must, at a future date, provide criteria for the exemption of small businesses and startups means that the bill's true scope is to be determined.

[XXVIII] Politicians participating in the Congressional testimonies involving Mark Zuckerberg were widely condemned for their lack of understanding of how the internet and internet-based companies work; Laura Manley, director of Harvard University's Technology and Public Purpose Project has similarly addressed this issue. Kang, Kaplan, and Fandos, "Knowledge Gap Hinders Ability of Congress to Regulate Silicon Valley"; Rampell, "Opinion | Our Politicians Have No Idea How the Internet Works"; Harvard Institute of Politics, *Big Tech and Democracy*.

[XXIX] As making recommendations to Congress does not constitute rulemaking, FTC would be free of the Magnuson-Moss constrains in doing so. However, if FTC promulgates regulations under Sec.4(a)(2), it would then be required to abide by Magnuson-Moss.

[XXX] While 5 U.S.C. § 522a(p) established Data Integrity Boards to provide oversight and ensure compliance with certain provisions of the Privacy Act, rather than being a separate regulatory entity, these boards were established by and inside of the agencies covered under the Act. Likewise, the Privacy Protection Study Commission lacked enforcement capabilities, and was instead focused on providing recommendations for protecting privacy.

disclosures of records. Sec.4 (b)(H) requires that paragraphs (1) through (12) of 5 U.S.C §552a(b) be incorporated as exceptions to the accounting requirement- paragraph (3) excludes disclosures under "routine use." The routine use exception would allow companies to argue that a core function of their business is collecting and sharing information with one another, thereby constituting routine use.

Privacy Bill of Rights Act

In April 2019 Sen. Markey (D-MA) unveiled the Privacy Bill of Rights Act, which he framed as necessary given that, "America's laws have failed to keep pace with the unprecedented use of consumers' data and the consistent cadence of breaches and privacy invasions that plague our economy and society."[207] According to the Senator's website, the Act claims five major provisions:[208]

1. Companies cannot use an individual's personal information in discriminatory ways.[209]
2. Companies must protect and secure individuals' personal information that they hold.[210]
3. FTC must establish a website informing consumers of their privacy rights and requires that companies use easy to read standardized short-form notices regarding their data collection, retention, and use practices.[211]
4. Companies may only collect the minimum data needed in order to provide the requested service or product.[212]
5. Both State attorney generals and individual private citizens may bring civil suit against violators of the Act.[213]

Establish auditing/reporting mechanism with Federal oversight	**Yes**	Not less frequently than every two years, FTC is to audit the privacy and security practices of companies that deal with confidentiality, integrity, and availability of personal information held by the company.[214] Should FTC deem appropriate, audits may be outsourced to an independent third party.[215]
Improve transparency for consumers	**Very high**	FTC must establish a centralized website informing consumers of their rights under the Act, and a second listing every data broker in America.[216] Companies must develop short-form notices, standardized by FTC, informing consumers about collection, use, and retention practices;[217] short-form notices must be clear, concise, well organized, and understandable written, complete; and cannot contain unrelated, confusing, or contradictory material.[218] Companies must, to the extent FTC deems appropriate, provide consumers access their information in a way that delineates between information collected to provide an individual with the desired product or service, and information collected and then sold to a third party.[219] Within 90 days of a request companies must provide a user with confirmation as to whether they retain information on that individual and a

Promulgate baseline data/information principles	**Yes**	description of said data.[220] Companies may not deidentify data held on an individual during the 90-day period, beginning when an individual makes a request pursuant to Sec. 6(a), preventing deidentification in order to circumvent a consumer's right to access, correct, and delete their data.[221] Companies must obtain opt-in approval from an individual in order to collect, use, retain, share, or sell said individual's personal data, allowing for the revocation of approval at any time.[222] Companies may not collect personal information that is beyond what is adequate, relevant, and necessary for the performance of the contract to which said individual is party, or to provide the requested product or service (data minimization).[223] Companies may not access an individual's information later than 90 days after the latest date on which a company concludes the performance of a contract, the company takes steps an individual would consider necessary in order to provide the requested service or product, or an individual terminates their contract.[224]
Enhance FTC rulemaking	**Yes**	Provides for APA rulemaking.[225]
Allow for civil penalties	**Yes**	The attorney general of a State may seek civil penalties.[XXXI]
Address FTC staffing and funding	**No**	N/A

Table 6 Privacy Bill of Right Act Evaluation

The Privacy Bill of Rights is the strongest of all alternatives analyzed in this report, being the only bill to address five of the six evaluative criteria. Two additionally noteworthy provisions are the prohibition on reidentifying personal information that has been deidentified and requiring that companies obtain opt-in permission.[226] However, certain aspects of these provisions and the exclusion of appropriations to facilitate enforcement preclude the Act from being the policy recommended by this report.

The Act's overall scope covers any company that "collects or otherwise obtains personal information," to include tech giants, BIAS providers, data brokers, small businesses, and startups.[227] The scope's vastness, coupled with the absence of appropriations for the Act's enforcement would overwhelm FTC and further diminish its enforcement capabilities.

[XXXI] The bill's actual text provides a State attorney general with the ability to take civil action to enjoin an action in violation of the bill; enforce compliance with the bill or appropriate regulation; obtain damages, restitution, or compensation for residents of the state; or obtain other relief considered appropriate by the court. This text provides for the authority to seek civil penalties. See Sec. 16(a) in Markey, Privacy Bill of Rights Act.

Sec. 5(e) alters the scope of the Act insofar as it pertains to the requirement that companies obtain opt-in consent from consumers before collecting, using, retaining, sharing, or selling an individual's information. This provision allows FTC to grant a specific company exception from the opt-in consent requirement based on 1) the privacy risks posed by the use of personal information possessed by a company, 2) the costs and benefits of the requirement to the company, 3) whether the collection and use of the information would be deemed necessary to carry out functions of the company,[XXXII] or 4) if the company de-identifies the data. The specific inclusion of the "costs and benefits" consideration would allow for the exemption of small businesses and start-ups, though the bill requires that the FTC individually grant companies exemptions rather than being able to do so based on predetermined guidelines such as revenues or size of user base. Tech giants, as defined by this report, may also try to abuse the costs and benefits provision, arguing that an opt-in consent requirement would be too costly to implement for companies who rely on targeted advertising as a major revenue source.[XXXIII]

Similarly, scope is detrimental with respect to the auditing function outlined in Sec. 13, as FTC does not have the resources needed to audit so many companies every two years. While there is a provision to outsource audits,[228] alleviating strain on FTC, PwC's auditing of Facebook, as discussed in the background section, shows that third parties audits are not by defaul, more reliable than self-regulation. While the outlined audit requirements are good, they do not allow specifically for the auditing of a company's data collection practices, leaving FTC or consumers with no way to ensure that companies are: truthful in their short-form notices;[229] honoring the opt-in choices of consumers;[230] transparent in their responses to requests for access, correction, and deletion of an individual's data;[231] or abiding by data minimization.[232]

The Act only allows for the attorney general of a State to seek civil penalties against first-time violators, forcing FTC to rely on consent orders. The same punitive damages issues raised for CONSENT apply here too. Individual citizens may also bring civil action against violators in either Federal or State courts.[233] The same issues regarding punitive damages arise for Federal court, while at least 19 states have implemented statutory limitations regarding the awarding of punitive damages.[234] Individual suits are likely of little deterrence for tech giants, given their ability to hire legions of top-tier corporate lawyers and drag cases on long after an individual plaintiff has run out of resources or energy to continue pursuing the case.

Policy Recommendation

Consumer Data Protection Act

In 2018 Sen. Wyden (D-OR) released a discussion draft of The Consumer Data Protection Act. Sen. Wyden directly addressed informational asymmetries, stating, "Americans know far too

[XXXII] These functions may include ensuring the security of the company's service; providing the service requested by the consumer, in a manner consistent with the context of the service provided; or those pertaining to payment for the requested service or product. See Sec. 5(e) in Markey, Privacy Bill of Rights Act.

[XXXIII] As targeting advertising necessitates that companies collect data from consumers in order to extrapolate the preferences of specific individuals. This argument would be applicable for companies such as Facebook and Google.

little about how their data is collected, how it's used and how it's shared," and that the Act would create "radical transparency for consumers."[235] The Act's goal is to give "FTC the authority to be an effective cop on the beat," providing the Commission with the tools and resources needed to protect Americans' privacy, instructing FTC to:[236]

1. Promulgate baseline privacy and cybersecurity standards;[237]
2. issue steep fines for first-time offenders and seek criminal penalties for senior executives;[238]
3. create a "Do Not Track" website that allows consumers to opt out of third-party tracking, while allowing companies to charge consumers seeking access to their products and services without having to opt-in to third-party tracking; [239]
4. require that companies provide consumers a mechanism through which to view what personal information a company holds on them, if said information was shared/sold/disclosed to third parties, and to challenge the accuracy of any such information;[240]
5. hire an additional 175 employees to enforce the Act and regulate the private data market;[241] and
6. require that companies conduct impact assessments in order to determine the impact on accuracy, fairness, bias, discrimination, privacy, and security, their automated decisions systems have.[242]

"Personal information" is defined as, "any information, regardless of how the information is collected, inferred, or obtained that is reasonably linkable to a specific consumer or consumer device.[243]

Establish auditing/reporting mechanism with Federal oversight	**Yes**	Certain companies must submit annual reports to FTC outlining their compliance with the Act[XXXIV]. Accompanying these annual reports must be a written statement signed by the company's executives certifying that the report is truthful and compliant with the reporting requirements of the Act.[XXXV]
Improve transparency for consumers	**High**	Companies must provide, at no cost and no later than 30 days after receiving written request, an individual with a reasonable means to review any stored personal information pertaining to them. Companies must also disclose: how and when the data was collected; a list of each person, partnership, or corporation with whom an

[XXXIV] Specifically, the Act requires that any company with +$1 billion in revenue who stores, shares, or uses personal information from more than 1 million consumers or consumer devices, or any company that stores, shares, or uses personal information from +50 million consumers or consumer devices submit reports to FTC detailing their compliance with the provisions outlined in Sec. 7(b)(1)(A)-(B). See Sec. 5(a)(1) in Wyden, Consumer Data Protection Act.

[XXXV] The Chief Executive Officer, Chief Technology Officer (or equivalent thereof), and Chief Information Security Officer (or equivalent thereof), are required to sign these reports. See Sec.5(a)-(b) in Wyden.

		individual's personal information was shared; any personal information stored by the company that the company itself did not collect, from whom that information was obtained, and why.[244] FTC must develop standards for which the above information is presented to consumers.[245]
Promulgate baseline data/information principles	**Yes**	Companies must: provide consumers with the option of opting-out of third-party data sharing arrangements;[246] within two years, establish and implement reasonable cybersecurity and privacy policies, practices, and procedures, in accordance with future regulations promulgated by FTC;[XXXVI] and, in accordance with regulations promulgated by FTC, establish and implement reasonable physical, technical, and organizational measures to ensure that technologies or products used, produced, sold, offered, or leased by the company are built and function consistently with reasonable data protection practices.[247]
Enhance FTC rulemaking	**Yes**	Provides for APA rulemaking.[XXXVII]
Allow for civil penalties	**Yes**	Revises the FTC Act such that FTC may assess civil penalties from companies engaged in unfair methods of competition, or unfair or deceptive business practices.[248] Violations of the Act are classified as an unfair or deceptive act or practice by the Act itself.[249] The Act allows for assessment of a civil penalty for a maximum sum that is the greater of: $50,000 per violation, taken as the aggregate sum of all violations; or, 4% total annual gross revenue of the violator for the prior fiscal year.
Address FTC staffing and funding	**Yes**	Establishes a Bureau of Technology headed by a chief technologist.[250] The Bureau's director is to appoint, without regard for civil service laws, 50 personnel with expertise in management, technology, digital design, user experience (UX), product management, software

[XXXVI] Sec. 7(b)(2) requires that in developing these regulations, FTC must consult the National Institute of Standards and Technology. See Sec. 7(b)(1)(A) in Wyden, Consumer Data Protection Act.

[XXXVII] Rather than establishing a standalone rulemaking section, the Act instead contains a provision in each individual section that gives FTC APA rulemaking authority for that specific section. See Sec. 5(a)(2), Sec. 6(a), and Sec. 7(b)(1) in Wyden, Consumer Data Protection Act.

		engineering, and related fields. Provides for the appointment of 100 additional personnel for the Division of Privacy and Identity Protection, and 25 additional personnel for the Division of Enforcement.[251] Authorizes whatever sum necessary to facilitate the above.[252]

Table 7 Consumer Data Protection Act Evaluation

The Consumer Data Protection Act is the only bill to address all six of the evaluative criteria, providing consumers with excellent privacy protection,[XXXVIII] while additional provisions further strengthen these protections. For these reasons, this report recommends the Act for establishing a non-industry-specific Federal privacy regulatory framework. As the Act is currently a discussion draft, and bills do undergo revision, this report also suggests seven revisions/additions that further enhance its effectiveness.

Analysis

The Act's scope covers any company FTC has jurisdiction over that 1) does not meet the gross receipts test by a factor of two, and 2) that had personal information on +1 million consumers or consumer devices in the most recent fiscal year.[XXXIX] The Act explicitly excludes data brokers.[253] Defining scope in this manner ensures the bill focuses on tech giants while protecting small-businesses and startups from the disproportionate regulatory costs they bare.

The Act requires that the standard of proof for what constitutes "substantial injury," which must be met in order for FTC to take enforcement action, is amended to allow for the consideration of the noneconomic impacts of privacy-related harms.[XL] This amendment makes the Act the only proposal analyzed to acknowledge the unique nature of privacy-related harms and that seeks to remedy current issues with the FTC Act's "unfairness" definition.

The Act's civil penalty provisions are the only ones analyzed that give FTC the direct ability to assess civil penalties from violators of the Act, providing for penalties at least 5x larger than those in the other bills. The Act further outperforms the others as it is the only one to allow FTC to assess penalties for first-time violators, providing for more effective remedy than the current consent order scheme. The Act is also the only one to include provisions for criminal penalties; executives who certify, or intentionally certify, the written statements accompanying annual reports knowing that the annual report does not satisfy the requirements outlined in Sec. 5 face

[XXXVIII] See Appendix VI for an aggregated overview of each bill's provisions.
[XXXIX] To reiterate, 26 U.S.C. § 448(c)(1) provides that corporations or partnerships with average annual gross receipts for the three-taxable-year period ending with the taxable year proceeding the current exceeding $25 million do not meet the gross receipts test.
[XL] This is done by amending the first sentence of 15 U.S.C. § 45(n) by inserting ", including those involving noneconomic impacts and those creating a significant risk of unjustified exposure of person information," after "cause substantial injury." See Sec. 3 in Wyden, Consumer Data Protection Act.

steep fines, jail time, or both.[XLI] Facebook's sending of unqualified personnel to testify in front of Parliament is indicative of the lack of accountability tech giant CEOs currently enjoy- the Act's criminal provisions serve to enhance accountability and deter noncompliance.

The National Institute of Standards and Technology, whose mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways the enhance economic security and improve our quality of life,"[254] must be consulted by FTC when promulgating regulations under Sec. 7. Companies affected by the bill can rest assured that regulations will be respectful of and acknowledge the fact that internet-age companies rely on user data in order to deliver their products and services. The NIST requirement means companies need not worry about stifling innovation or being regulated into bankruptcy. Similarly, allowing companies to charge a fee for access to their product or service, should consumers opt out of data sharing, allows companies to minimize the economic impact of new regulations.[255]

The Act also requires the standardization of Application Programming Interfaces and the forms used to provide consumers with information under Sec. 6-7.[256] Standardization makes it easier for consumers to alter their privacy and "Do Not Track" settings, dispute information held on them, or obtain access to any such information, as these processes would be standardized across companies. Standardized APIs would also likely become an industry-wide best practice. NIST and relevant stakeholders must be consulted in the development of API standards, again alleviating concerns of regulatory overburden.

Recommended Changes

This report recommends seven changes/additions to the Act:

1. The Act requires that companies conduct automated decision system and data protection impact assessments of high-risk automated decision systems, making it the only bill to address the public interest harms first raised by the Obama White House.[257] However, the Act does not require that assessments be provided to FTC, and leaves to the discretion of the company whether assessments are made public.[258] While mandating that assessments be made public may incentivize companies to hide damaging findings, these reports should be made confidentially available to FTC in order to ensure that any public interest harms are appropriately addressed.

2. The reporting mechanism provided for in the Act is strong but could be improved by mandating that companies also report the specific methods they use to collect data,

[XLI] Under Sec. 5(b)(1), any individual who certifies an accompanying statement knowing that an annual report does not meet the requirements outlined in Sec. 5(b) and Sec. 5(c) faces fines up to $1 million or 5% of the largest amount of compensation the individual received in the previous three-year period from the company, imprisonment of up to 10 years, or both. The same section provides for fines of up to $5 million or 25% of the largest amount of compensation the individual received in the previous three-year period from the company, or imprisonment of up to 20 years, or both, for any individual who *intentionally* certifies an accompanying statement knowing that an annual report does not meet the requirements outlined in Sec. 5(b) and Sec. 5(c). See § 1352 (d) paragraphs (1) and (2) in Wyden.

addressing privacy-related harms that occur in the information collection phase.[XLII] Enabling FTC to conduct audits of the provided annual reports would add a further level of consumer protection, dramatically reduce informational asymmetries, and allow FTC to ensure that companies are truthful in their reporting. Provided that a company intentionally collected data in a certain manner, it is possible to audit what is being collected and how, especially given that the Act requires companies adopt standardized APIs.[XLIII] However, further work must go into determining whether or not special queries or investigative methods need to be designed for this task, or if this is financially feasible.[XLIV]

3. The inclusion of "reasonably linkable to a specific consumer or consumer device" in the definition of "personal information" infers that deidentified/anonymous information is not within the purview of the Act.[259] FTC may also grant a company exemption from the outlined opt-out requirements if a company deidentifies personal information before sharing it.[260] The Act should consider two provisions from the Consumer Privacy Bill of Rights: 1) Sec. 7's prohibition on reidentifying deidentified data; and 2) Sec. 6(c)'s prohibition of deidentifying data after a consumer requests to see what information a company holds on them, in order to avoid disclosing said information to consumers.

4. When promulgating regulations under Sec. 7, FTC and NIST should assess the feasibility of a data minimization regulation similar to Sec. 12 of the Consumer Privacy Bill of Rights. Such a provision would further protect consumers from corporate overreach, while still allowing companies to deliver user-specific products or services, such as real-time driving directions. Such a regulation may be economically viable given that the Act already allows companies to assess a fee for access to their products or services should consumers opt out information sharing.[261]

5. While notice provided to consumers, pursuant to a request to access information held on them, is required to be "clearly and concisely" presented,[262] the Act does not require that privacy policies must be easily understandable for consumers. The Act would do well to borrow from the Consumer Privacy Bill of Rights, which requires that companies provide consumers with short-from notices about the collection, retention, use, and sharing of personal information. These notices must be clear, concise, well-organized, understandably written, and complete; free of unrelated, confusing, or contradictory materials; and in a format that is prominent and easily accessible, of reasonable length, and clearly distinguishable from other matters; and standardized.[263] It may also be desirable to alter the scope of this section such that it is inclusive of all companies that are required to provide consumers with privacy policies.

[XLII] Such a provision is not included in the Act as written, however the data collection principles to be promulgated under Sec. 7(b)(1)(A)-(B) may eventually address this directly.

[XLIII] Given that APIs include specifications regarding data structures, routines, variables, or object classes, it is likely possible that FTC can develop a program or algorithm to fulfill this function.

[XLIV] In order to sift through the datasets of a company, an automated program would likely need a high-performance computing (supercomputer) cluster running a big data infrastructure- this may be outside of financial feasibility for FTC.

6. The Act should require that consumers opt-in to allowing a company to share their personal information, rather than opt-out, as opt-out schemes have been criticized as unfairly burdening individuals to ensure that companies responsibly share their personal information, rather than companies themselves.[264]

7. Amending 15 U.S.C § 45(n) to include "noneconomic impacts and those creating a significant risk of unjustified exposure of personal information" when establishing a standard of proof for injury would be more effective if the Act defined these impacts or provided examples of them in Sec. 2 (Definitions).[265] Doing so would prevent future debate over whether an outcome is a detrimental noneconomic impact resulting in injury.

Validation

Sen. Wyden's draft has already attracted praise from many sources, including advocacy group Consumers Union, search engine DuckDuckGo CEO Gabriel Weinberg, and four former FTC chief technologists.[266] Notably, the Act is the only bill to receive support from former FTC executives.

Globally, comprehensive internet privacy legislation is still in its infancy, an unsurprising fact given that the internet as we know it is still a relatively new platform. Nonetheless, in 2016 the European Union signed into law the General Data Protection Regulation (GDPR),[267] a bill to which the Consumer Data Privacy Act has been likened to by cybersecurity consultants and industry publications.[XLV] Others even suggest that the Act is more comprehensive than GDPR, especially in regards to enforcement, with tech expert and journalist Robert Hackett concluding, "if GDPR has teeth, Wyden's proposal has fangs."[268] Appendix VII provides an overview of specific similarities between the bills. Shortly after GDPR's passing California signed its own equivalent bill, the California Consumer Privacy Act, which will go into effect January 2020. [269]

Like the Act, GDPR's central focus is on tech giants, however it has also received criticism for disadvantaging small businesses/start-ups;[270] discussed above, the Act's scope resolves this problem by exempting smaller companies. According to surveys among CEOs, CIOs, CTOs, and risk officers, it is estimated that GDPR compliance will cost U.S. companies $41.7 billion.[271] Given similarities with the Consumer Data Protection Act, GDPR-compliant companies will have already built much of the infrastructure/capacity needed to comply with the Act. While critics claim it is unwise to regulate an industry as young as the internet,[272] GDPR shows that regulations can be implemented without adversely disrupting tech giants, many of whom waited until the last minute to become compliant.[273]

[XLV] For an overview of specific similarities, see Appendix VII. CSPi, "What Is the Latest Consumer Data Protection Act That Everyone Is Talking About?"; Green, "Wyden's Consumer Data Protection Act: How to Be Compliant"; Davis, "Proposed Privacy Bill Mirrors GDPR, Adds Jail Time for Lying CEOs"; CipherCloud, "The New Consumer Data Protection Act from Senator Ron Wyden from Oregon."

On February 26, 2019, the European Data Protection Board (EDPB) issued a review of the GRPD's implementation and enforcement in its first year of life.[XLVI] EDPB concluded "GDPR works quite well [in practice]."[274] While critics claim that GDPR has largely failed to take punitive action against violators,[275] Mathais Moulin, head of France's data privacy agency, CNIL, states that GDPR's first year "should be considered a transitional year," as regulators spent much of the year finalizing their rules and approaches, and focusing on closing out data/privacy investigations that originated prior to GDPR's enactment.[276]

Despite being a "transitional year," GDPR's effectiveness is seen in the decrease in demand for targeted/behavioral advertisements in Europe, which in some cases dropped by 25-40% immediately after the regulation came into effect; [277] three months after the bill, spending on ads increased, but still resulted in companies spending 20-30% less than before GDPR.[278] Decreased spending on targeted ads shows GDPR works, as companies such as Facebook and Google, both advertising market leaders, are now restricted in how they collect, use, and share consumers' information. GDPR's effectiveness is further exemplified through companies' adherence to the Regulation's breach reporting requirements; a spokesman from the UK Information Commissioner's Office called the increase of breach reports, up ~89% from the year before GDPR came into force, "massive."[XLVII]

Finally, that both the European Union and State of California have passed similar legislation is evidence that it the Consumer Data Protection Act is politically feasible, especially given the government's passing of previous privacy legislation (Privacy Act, HIPAA, GBLA, and FCRA). That there are currently five major legislative proposals further suggests that the political climate is right for a Federal privacy framework.

Conclusion

In 1974 private industry argued for their exclusion from the Privacy Act on the grounds that there was little evidence of abuses in private sector personal information practices. Similarly, lawmakers have long been cautious of regulating the internet sector, believing that regulation would stifle innovation. Today, Americans scarcely go a week without turning on the news to find that their privacy has again been disregarded by tech giants in their quest for ever-increasing profits. The lack of a comprehensive privacy framework in the United States has allowed tech giants to make their own rules, in their own best interests, at the expense of the consumer. Allowing companies to operate in this manner has resulted in a market failure, which FTC is currently unable to adequately address given a number of institutional constraints. The Data Care Act, CONSENT Act, ADD Act, and Privacy Bill of Rights Act all seek to establish a Federal privacy framework, but fall short of the evaluative criteria considered necessary by this report to

[XLVI] Though calling itself the first annual report, the report actually chronicles the first 9 months of GDPR's life. European Data Protection Board, "First Overview of the GDPR."

[XLVII] The 89% figure was calculated using 19,000 cases (taken as the average of "18,000 to 20,000") as the figure for pre-GDPR breach reporting, and 36,000 (UK Information Commissioner's Office estimate for 2019 breach report figures) as the 2019 figure. See Hill, "Year 1 of GDPR."

do so. While still a discussion draft, Sen. Wyden's Consumer Data Protection Act establishes a reporting mechanism with Federal oversight, improves transparency for consumers, promulgates baseline data collection principles, allows FTC to utilize APA rulemaking, provides for the assessment of steep civil penalties, and addresses staffing and funding issues at FTC. As such, this report recommends that Congress adopt the Consumer Data Protection Act with the recommended changes in order to establish a non-industry-specific privacy regime to ameliorate the above-mentioned failures, and to ensure that Americans enjoy their constitutional right to privacy.

Appendix I

Overview of Broadband Internet Access Service (BIAS) Providers and Data Brokers

BIAS Providers- "Owners of physical networks- known as broadband internet access service (BIAS) providers. BIAS providers, situated as the consumer's route to the internet as they are, necessarily gain access to a universe of sensitive personal data including any internet domains and unencrypted URLs the consumer may have visited- which can readily be used to infer the consumer's interests and preferences. These firms, the wireline leaders among them in the United States being AT&T, Comcast, Verizon, enjoy tremendous market power in the regions in which they operate. Meanwhile, they are increasingly investing in the digital advertising ecosystem because they see synergies between their data collection practices and the core resources needed to succeed in digital advertising."[XLVIII]

Data Brokers- Integral to the "big data" economy, these entities exist to buy and sell consumer data from numerous sources, often without the knowledge or consent of the consumer who created the data, as these firms do not directly interact with consumers.[279] Data brokers aggregate data in order to create digital dossiers on individual consumers, which are then sold to other companies. The scope of their operations is massive, with one company, Acxiom, claiming to have over 3,000 data segments for nearly every American consumer.[280]

[XLVIII] Excerpt from Ghosh and Scott, "Digital Deceit II," 23–24.

Appendix II

Abridged Overview of Solove's Privacy Taxonomy[XLIX]

According to leading privacy theorist Daniel J. Solove, there are four categories of activities with respect to privacy that may result in harm to consumers: 1) information collection, 2) information processing, 3) information dissemination, and 4) invasion.

Information Collection	
Harm	**Problem**
Surveillance: watching, listening to, recording an individual's activities	• Can lead to feelings of anxiety and discomfort if persistent. • Constitutes a lack of respect for consumers as autonomous persons. • May lead to societal self-censorship and inhibition. • Contradicts the Fourth Amendment right to a reasonable expectation of privacy.

Information Processing	
Harm	**Problem**
Aggregation: combining separate pieces of information about an individual	• Aggregated information can produce facts individuals didn't expect to reveal when data was first collected. • Assists in creating a comprehensive dossier or "digital person" mirroring an actual individual. • Provides the aggregator increased power over the individual.
Identification: linking information to a particular individual	• Links a "digital person" to an actual person, regardless of whether that person wishes to be affiliated that that "digital person." • Inhibits one's ability to be anonymous or pseudonymous.
Insecurity: glitches in data protection, security lapses, data abuses, illicit uses of personal information	• Stolen information dossiers can lead to identity theft, exposing individuals to potential future harm.

[XLIX] The taxonomy in its entirety can be found at Solove, *Understanding Privacy*, chap. 5.

	• Violates individuals' interest in avoiding disclosure of their personal matters. • A company violating their own privacy policy is an "unfair and deceptive act," per FTC.
Secondary Use: using data not within the context consented to by an individual	• Data is used in a manner not consistent with what an individual had consented to or that they may find undesirable. • Constitutes a possible breach of confidentiality. • Individuals lose trust in companies; thwarts expectations about how data they provide will be used. • Rarely mentioned in privacy policies; precludes individual from making informed decisions about their privacy, leading to one-sided bargain between individuals and companies (information asymmetry).
Exclusion: not allowing individuals to know what information others possess on them or affording them the opportunity to participate in its handling or use	• Reduces accountability of companies. • Precludes individual from making informed decisions about their privacy, leading to one-sided bargain between individuals and companies/information asymmetry. • Divests individuals of control over their lives, given the importance of personal information in decision making.

Information Dissemination	
Harm	**Problem**
Breach of Confidentiality: Breaking a promise to keep information confidential	• Betrayal/violation of an individual's trust. • Context dependent, may be an unfair or deceptive practice.
Disclosure: revealing information that affects an individual's reputation	• Violates Supreme Court-recognized right to privacy. • Can threaten an individual's safety. • Prevent individuals from engaging in activities that promote self-development. • Can restrict free speech. • Inhibits freedom of association. • Makes individuals vulnerable to irrational judgement based on stereotypes and

	misinformation; distorts ability to accurately assess an individual. • May penalize individuals for things not within their control. • Spreads information outside of expected boundaries.
Increased Accessibility: amplifying the accessibility of information	• Heightens the risk of disclosure. • Information can be readily exploited for purposes other than those consented to by an individual at the time of collection.
Appropriation: using consumers' data to serve another's interests	• Commercialization of an aspect of one's personality is an affront to their dignity. • The individual loses the ability to control how they are presented to others; impinges on an individual's freedom in authorship of own narrative.

Invasion	
Harm	**Problem**
Intrusion: invasions or incursions into one's life	• Interrupts an individual's activities through the unwanted presence or activities of another. • Interferes with an individual's solitude. • Can lead to feelings of anxiety and discomfort if persistent. • Lack of respect for consumer as an autonomous person. • May lead to self-censorship and inhibition. • Contradicts the Fourth Amendment right to a reasonable expectation of privacy.
Decisional Interference: incursion into a consumer's decisions regarding their private affairs	• Violates the autonomy of an individual and their independence when making certain decisions. • Violates the "right to be left alone."

Appendix III

Provisions Afforded by Industry-Specific Laws and The Privacy Act of 1974

HIPAA:

The "Privacy Rule" is located at 45 CFR §160 and 45 CFR §164 (A) and (E).[281] The U.S. Department of Health & Human Services identifies nine general categories of privacy standards: 1) consent,[282] 2) sharing of the minimum necessary information,[283] 3) oral communications,[284] 4) business associates,[285] 5) parents and minors,[286] 6) health-related communications and marketing,[287] 7) research,[288] 8) restrictions on government access to health information,[289] and 9) payment.[290] Together, these categories:

1. Give patients more control over their health information;
2. set boundaries on the use and release of records;
3. establish record safeguards providers must follow;
4. hold violators accountable with civil and criminal penalties if they violate a patient's privacy rights;
5. enable patients to find out how their information may be used and what disclosures have been made;
6. limit the release of information to the minimum needed to perform a function (data minimization); and
7. give patients the right to access their records and request corrections.[291]

FRCA:

The Fair Credit Reporting Act:

1. Prevents information from being provided to unwarranted parties;
2. requires companies to investigate disputed information; and
3. requires individuals to be notified of adverse action taken on the basis of CRA-possessed information.[292]

GLBA:

The Gramm-Leach-Bliley Act:

1. Requires financial institutions to develop procedures to keep personal information secure and confidential;
2. requires financial institutions to provide consumers notice of their information sharing policies;
3. allows consumers to opt out of certain types of sharing;
4. prohibits financial institutions from disclosing access codes or account numbers to nonaffiliated third parties; and

5. prohibits collecting personal information under certain false pretenses.[293]

The Privacy Act of 1974:

The Privacy Act's code of fair information practices:

1. Requires written request/consent from an individual before disclosing any record pertaining to said individual;[294]
2. requires agencies to keep records of certain disclosures and inform individuals of said disclosures;[295]
3. gives individuals access to records held on them;[296]
4. allows individuals to request amendments to their records;[297]
5. mandates that agency records meet certain requirements for:[298]
    a. relevancy;
    b. accuracy;
    c. disclosure;
    d. publication annually of their, character, and accessibility;
    e. confidentiality safeguards;
6. requires agencies to establish rules pertaining to notice, access, and amendment;[299] and
7. provides civil remedy for violations of the act.[300]

Privacy Act Amendments:

Together, the 1988 and 1990 amendments to 5 U.S.C § 552a require that any Federal agency seeking to share data with another agency or non-Federal agency engage in written agreements that must include:

1. The purpose and legal authority for sharing;[301]
2. justification for sharing intended results;[302]
3. a detailed description of the records to be shared;[303]
4. procedures for notifying affected individuals, verifying accuracy of the records, keeping records secure and current and regulating the use of the results of data sharing programs;[304]
5. assessments of record accuracy;[305] and
6. permission for the Comptroller General to have access to all records deemed necessary to monitor compliance.[306]

Appendix IV

Excerpt from Preliminary Transcript of Mark Zuckerberg Testimony to House of Representatives Committee on Energy and Commerce[307]

The Chairman: The gentleman yields back the balance of his time. The gentlelady from California, Ms. Matsui, is recognized for 4 minutes.

Ms. Matsui: Thank you, Mr. Chairman. And welcome, Mr. Zuckerberg. Thank you very much here. You know, I was just thinking about Facebook and how you developed your platform, first from a social platform amongst friends and colleagues and joining a community. And a lot of that was based upon trust, because you knew your friends, right? But that evolved into this business platform, and one of the pillars still was trust. And I think everyone here would agree that trust is in short supply here, and that is why we are here today.

Now, you have constantly maintained that consumers own the data they provided to Facebook and should have control over it. And I appreciate that, and I just want to understand more about what that means.

To me, if you own something, you ought to have some say about how and when it is used, but, to be clear, I don't just mean pictures, email addresses, Facebook groups, or pages. I understand the data and the information consumers provided to Facebook can be and perhaps is used by algorithms to form assumptions and inferences about users to better target ads to the individuals.

Now, do you believe that consumers actually own their data even when that data has been supplemented by a data broker, assumptions algorithms have made about that user, or otherwise?

And this is kind of the question that Mrs. Blackburn has come up with, our own comprehensive profile, which is kind of our virtual self.

Mr. Zuckerberg: Congresswoman, I believe that people own all of their own content. Where this gets complicated is, let's say I take a photo and I share it with you. Now, is that my photo, or is it your photo? I would take the position that it is our photo, which is why we make it so that I can bring that photo to another app if I want but you can't. But --

Ms. Matsui: Well, once it gets to the data broker, though -- so there are certain algorithms and certain assumptions made. What happens after that?

Mr. Zuckerberg: Sorry, can you clarify that?

Ms. Matsui: Well, what I mean is that, if you supplement this data, you know, you say you are owning it, but you supplement this when other data brokers, you know, use their other algorithms to supplement this and make their own assumptions, then what happens there? Because that is, to me, somebody else is taking that over. How can you say that we own that data?

Mr. Zuckerberg: Congresswoman, all the data that you put in, all the content that you share on Facebook is yours. You control how it is used. You can remove it at any time. You can get rid of your account and get rid of all of it at once. You can get rid of specific things.

Ms. Matsui: But you can't claw it back once it gets out there, right? I mean, that is really -- we might own our own data, but once it is used in advertising, we lose control over it. Is that not right?

Mr. Zuckerberg: Congresswoman, I disagree with that, because one core tenet of our advertising system is that we don't sell data to advertisers. Advertisers don't get access to your data.

There is a core misunderstanding about how that system works, which is that -- let's say, if you are a shop and you are selling muffins, right, you might want to target people in a specific town who might be interested in baking or some demographic. But we don't send that information to you; we just show the message to the right people. And that is a really important, I think, common misunderstanding of how this system works.

Ms. Matsui: Yeah, I understand that, but Facebook sells ads based, at least in part, on data users provide to Facebook. That is right. And the more data that Facebook collects, it allows you to better target ads to users or classes of users.

So, even if Facebook doesn't earn money from selling data, doesn't Facebook earn money from advertising based on that data?

Mr. Zuckerberg: Yes, Congresswoman, we run ads. The business model is running ads. And we use the data that people put into the system in order to make the ads more relevant, which also makes them more valuable. But what we hear from people is that, if they are going to see ads, they want them to be good and relevant.

Ms. Matsui: But we are not controlling that data?

Mr. Zuckerberg: No, you have complete control over that.

The Chairman: The gentlelady's time has expired.

Appendix V

Excerpt from Transcript of Mark Zuckerberg's Testimony to the Senate Committees on the Judiciary and Commerce, and Science and Transportation[308]

MORAN: Mr. Chairman, thank you. Mr. Zuckerberg, thank you for your — I'm over here. Thank you for your testimony and thank you for your presence here today. On March the 26th of this year, the FTC confirmed that it was investigating Facebook to determine whether its privacy practices violated the FTC Act or the consent order that Facebook entered into with the agency in 2011.

I chair the Commerce committee — subcommittee that has jurisdiction over the Federal Trade Commission. I remain interested in Facebook's assertion that it rejects any suggestion of violating that consent order. Part two of that consent order requires that Facebook, quote, "clearly and prominently" display notice and obtain users' affirmative consent before sharing their information with, quote, "any third party.?

My question is how does the case of approximately 87 million Facebook friends having their data shared with a third party due to the consent of only 300,000 consenting users not violate that agreement?

ZUCKERBERG: Well, Senator, like I said earlier, I mean our view is that — is that we believe that we are in compliance with the consent order, but I think we have a broader responsibility to protect people's privacy even beyond that. And in this specific case, the way that the platform worked, that you could sign into an app and bring some of your information and some of your friends' information is how we explained it would work. People had settings to that effect. We explained and — and they consented to — to it working that way. And the — the system basically worked as it was designed.

The issue is that we designed the system in a way that wasn't good. And now we — starting in 2014, have changed the design of the system to that that way it just massively restricts the amount of — of data access that a developer could get.

(CROSSTALK)

MORAN: The — I'm sorry, the 300,000 people, they were treated in a way that — it was appropriate; they consented. But you're not suggesting that the friends consented?

ZUCKERBERG: Senator, I believe that — that we rolled out this developer platform, and that we explained to people how it worked, and that they did consent to it. It — it makes, I think, to — to go through the way the platform works. I mean, it's — in 2007, we — we announced the Facebook developer platform, and the idea was that you wanted to make more experiences social, right?

So, for example, if you — like, you might want to have a calendar that can have your friends' birthdays on it, or you might want your address book to have your friends' pictures in it, or you might want a map that can show your friends' addresses on it. In order to do that, we needed to build a tool that allowed people to sign in to an app and bring some of their information, and some of their friends' information, to those apps. We made it very clear that this is how it worked, and — and when people signed up for Facebook, they signed up for that as well.

Now, a lot of good use cases came from that. I mean, there were games that were built. There were integrations with companies that, I think, we're familiar with, like Netflix and Spotify. But over time, what became clear was that that also enabled some abuse. And that's why in 2014, we took the step of changing the platform. So now, when people sign in to an app, you do not bring some of your friends' information with you. You're only bringing your own information and you're able to connect with friends who have also authorized that app directly.

Appendix VI

Aggregated Summary of Bill Provisions

	Data Care Act	CONSENT Act	ADD Act	Privacy Bill of Rights Act	Consumer Data Protection Act
Establish auditing/reporting mechanism with Federal oversight	No	No	No	Yes	Yes
Improve transparency for consumers	Very Low	Moderate Improvement	Very Low	Very High	High
Promulgate baseline data/information principles	No	Yes	Yes	Yes	Yes
Enhance FTC rulemaking	Yes	Yes	No	Yes	Yes
Allow for civil penalties	Yes	Yes	No	Yes	Yes
Address FTC staffing and funding	No	No	No	No	Yes

Appendix VII

GDPR and the Consumer Data Privacy Act

	GDPR	Consumer Data Privacy Act
Scope (company): GDPR does not differentiate between companies of different sizes[L]	Applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means, of personal data which form part of a filing system or are intended to form part of a filing system.[309]	Any entity over which FTC has jurisdiction with more than $50 million in average annual gross receipts for the 3-taxable-year period preceding the fiscal year; had personal information on more than 1 million consumers and consumer devices; and is not a data broker.[310]
Scope (data): Both concerned with personally-identifiable information.	Personal data is any information relating to an identified individual or identifiable natural person.[311]	Personal information is any information, regardless of how it is collected, inferred, or obtained that is reasonably linkable to a specific consumer or consumer device.[312]
Penalties for violators	Administrative fines with a maximum penalty of up to €20 million or 4% of total worldwide annual turnover for the preceding financial year, whichever is higher.[313]	Assessment of a civil penalty for a maximum sum that is the greater of: $50,000 per violation, taken as the aggregate sum of all violations; or, 4% total annual gross revenue of the violator for the prior fiscal year.[314]
Compliance officers	Companies must designate a data protection officer whose job is to ensure compliance with GDPR.[315]	Companies must designate at least one employee, who reports directly to an employee acting in an executive capacity, who is responsible for compliance with the Act.[316]

[L] While not a similarity, as scope pertains to types of entities affected as well as types of data, it is necessary to differentiate between the two.

Promulgate baseline collection principles	Requires that Member States, supervisory authorities, and the Board of the Commission develop and promulgate of codes of conduct companies must adhere to.[317]	Within two years, establish and implement reasonable cybersecurity and privacy policies, practices, and procedures in accordance with future regulations promulgated by FTC.[318]
Consent	Individuals must consent to companies processing their personal data. Consent must be opt-in rather than opt-out.[319]	Creates a "Do Not Track" website where consumers can opt-out of allowing companies to share their information with third parties.[320] As written, does not explicitly require that consumers opt-in to the processing of their information by companies with which they are directly engaged.
Transparency	Requires that any information and communication relating to the processing of personal information be easily accessible, easily understood, and use clear and plain language.[321] Companies must provide to individuals certain information when their data are collected both directly and indirectly.[322] Individuals must, upon request, be granted confirmation as to whether a company holds data on them, and if so, access to that data and certain information regarding it.[323]	Companies must provide, at no cost and no later than 30 days after receiving written request, an individual with a reasonable means to review any stored personal information pertaining to that consumer. Companies must also disclose: how and when the data was collected; a list of each person, partnership, or corporation with whom an individual's personal information was shared; any personal information stored by the company that the company itself did not collect, and information as to from whom that information was obtained, and why.[324]
Right to correct inaccurate information	Individuals have the right to correct inaccurate personal data concerning him or her held by a company, without undue delay.[325]	Companies must correct personal information held on an individual after investigating a challenge by said individual to the information's accuracy.[326]

Enforcement	Each Member Nation is to establish/provide an independent public authority responsible for monitoring compliance with GDPR within its territory.[327]	FTC is the United States' independent public authority responsible for the Act.
Federally overseen reporting/auditing mechanisms	Each independent public authority is given the power to carry out investigations in the form of data protection audits.[328]	Certain companies must submit annual reports to FTC outlining their compliance with the Act[LI]. Accompanying these annual reports must be a written statement signed by the company's executives certifying that the report is truthful and compliant with the reporting requirements of the Act.[LII]

[LI] Specifically, the Act requires that any company with +$1 billion in revenue who stores, shares, or uses personal information from more than 1 million consumers or consumer devices, or any company that stores, shares, or uses personal information from +50 million consumers or consumer devices submit reports to FTC detailing their compliance with the provisions outlined in Sec. 7(b)(1)(A)-(B). See Sec. 5(a)(1) in Wyden, Consumer Data Protection Act.

[LII] The Chief Executive Officer, Chief Technology Officer (or equivalent thereof), and Chief Information Security Officer (or equivalent thereof), are required to sign these reports. See Sec.5(a)-(b) in Wyden.

Notes

[1] House of Commons Digital, Culture, Media and Sport Committee, "Disinformation and 'Fake News': Final Report," 42.
[2] Wyden, Consumer Data Protection Act.
[3] Harvard Institute of Politics, *Big Tech and Democracy*.
[4] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," 37; Ghosh and Scott, "Digital Deceit II," 22.
[5] Federal Trade Commission, "Preliminary FTC Staff Report," I.
[6] Narayanan, "Privacy and the Market for Lemons, or How Websites Are Like Used Cars." Narayanan is an associate professor of computer science at Princeton University specializing in information privacy and security.
[7] Ghosh and Scott, "Digital Deceit II," 49.
[8] Ghosh and Scott, 39–40.
[9] Ghosh and Scott, "Digital Deceit II," 31.
[10] Hoofnagle and Whittington, "Free: Accounting for the Costs of the Internet's Most Popular Price," 639.
[11] Ghosh and Scott, "#Digital Deceit," 6.
[12] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," 2.
[13] Schlesinger and Andrea Day, "Most People Just Click."
[14] Acquisti, Taylor, and Wagman, "The Economics of Privacy," 483.
[15] Harvard Institute of Politics, *Big Tech and Democracy*.
[16] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," 17; Ghosh and Scott, "Digital Deceit II," 25 & 59.
[17] Ghosh and Scott, "Digital Deceit II," 26–27.
[18] Harvard Institute of Politics, *Big Tech and Democracy*.
[19] Ghosh and Scott, "Digital Deceit II," 36.
[20] Madden and Rainie, "Americans' Attitudes About Privacy."
[21] Reagan, *Legislating Privacy*, 23.
[22] Ribak, "'Privacy Is a Basic American Value:' Globalization and the Construction of Web Privacy in Israel," 3.
[23] Madden and Rainie, "Americans' Attitudes About Privacy."
[24] Madden and Rainie.
[25] Gramlich, "10 Facts about Americans and Facebook."
[26] "The State of Privacy in Post-Snowden America."
[27] Reagan, *Legislating Privacy*, 25.
[28] Senate Committee on Government Operations and House Committee on Government Operation, "Legislative History of the Privacy Act of 1974, S. 3418 (Public Law 93-579)," 89.
[29] Rothman, "The Surprising History Behind America's Stand Your Ground Laws."
[30] Warren and Brandeis, "The Right to Privacy," 220.
[31] Pound, "Interests of Personality," 362.
[32] Igo, *The Known Citizen*, 35.
[33] Warren and Brandeis, "The Right to Privacy," 198–99.
[34] Warren and Brandeis, 193.
[35] Warren and Brandeis, 193.

[36] Wex Legal Dictionary, "Fourth Amendment."
[37] Warren and Brandeis, "The Right to Privacy," 195.
[38] Wex Legal Dictionary, "Privacy."
[39] Wex Legal Dictionary.
[40] "Katz v. United States, 389 U.S. 347 (1967)."
[41] Cornell Law School Legal Information Institute, "Katz v. United States."
[42] Turley, "Supreme Court's GPS Case."
[43] "Carpenter v. United States."
[44] Wessler, "The Supreme Court's Groundbreaking Privacy Victory for the Digital Age."
[45] Reagan, *Legislating Privacy*, 26.
[46] Reagan, 8.
[47] Reagan, 71.
[48] Igo, *The Known Citizen*, 223.
[49] Igo, 223.
[50] Privacy Protection Study Commission, "Personal Privacy in an Information Society: The Report of The Privacy Protection Study Commission," 497.
[51] U.S. House, H.R.3103 - Health Insurance Portability and Accountability Act of 1996.
[52] "Fair Credit Reporting Act 15 U.S.C. § 1681."
[53] U.S. Senate, S.900 - Gramm-Leach-Bliley Act.
[54] "What Is HIPAA?"
[55] U.S. Department of Health & Human Services Office of the Assistant Secretary for Planning and Evaluation, "Standards for Privacy of Individually Identifiable Health Information."
[56] Electronic Privacy Information Center, "The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report."
[57] Electronic Privacy Information Center.
[58] Electronic Privacy Information Center, "The Gramm-Leach-Bliley Act."
[59] Electronic Privacy Information Center.
[60] Electronic Privacy Information Center.
[61] Privacy Protection Study Commission, "Personal Privacy in an Information Society: The Report of The Privacy Protection Study Commission," 497.
[62] Reagan, *Legislating Privacy*, 71.
[63] United States Department of Justice Office of Privacy and Civil Liberties, "Overview of The Privacy Act of 1974: Policy Objectives."
[64] P. 13, Title II Sec. 201(a) in, Senate Committee on Government Operations and House Committee on Government Operation, "Legislative History of the Privacy Act of 1974, S. 3418 (Public Law 93-579)."
[65] United States Department of Justice Office of Privacy and Civil Liberties, "Overview of The Privacy Act of 1974"; Reagan, *Legislating Privacy*, 78.
[66] United States Department of Justice Office of Privacy and Civil Liberties, "Overview of The Privacy Act (2015 Edition)," 1.
[67] United States Department of Justice Office of Privacy and Civil Liberties, "Overview of The Privacy Act of 1974"; United States Department of Justice Office of Privacy and Civil Liberties, "Overview of The Privacy Act of 1974: Policy Objectives."
[68] U.S. Senate, S.3418 - An Act to amend title 5, United States Code, by adding a section 552a, to safeguard individual privacy from the misuse of Federal records, to provide that individuals be

granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes.
[69] Electronic Privacy Information Center, "The Privacy Act of 1974."
[70] United States Department of Justice Office of Privacy and Civil Liberties, "Overview of The Privacy Act (2015 Edition)," 1.
[71] U.S. Senate, S.496- Computer Matching and Privacy Protection Act of 1988.
[72] Government Printing Office.
[73] U.S. House, H.R. 5835- Omnibus Budget Reconciliation Act of 1990.
[74] Sec. 4 of Pub. L. No. 101–508.
[75] Sec. 4 2(b)(3)(E) of Pub. L. No. 101–508.
[76] Reagan, *Legislating Privacy*, 78.
[77] Reagan, 78.
[78] Hitlin and Rainie, "Facebook Algorithms and Personal Data."
[79] "The Top 500 Sites on the Web."
[80] House of Commons Digital, Culture, Media and Sport Committee, "Disinformation and 'Fake News': Final Report," 42.
[81] House of Commons Digital, Culture, Media and Sport Committee, 14.
[82] Rosenberg, Confessore, and Cadwalladr, "Consultants Exploited Facebook."
[83] Cadwalladr and Graham-Harrison, "50 Million Profiles Harvested."
[84] Kozlowska, "The Cambridge Analytica Scandal Affected Nearly 40 Million More People than We Thought."
[85] Cadwalladr and Graham-Harrison, "50 Million Profiles Harvested."
[86] Cadwalladr and Graham-Harrison, "50 Million Profiles Harvested."
[87] Hern, "Facebook: Washington DC Sues Tech Giant over Cambridge Analytica Data Use."
[88] Wong, "Facebook Acknowledges Concerns over Cambridge Analytica Emerged Earlier than Reported"; Damian Collins, Twitter post, March 21 2019, 11:01 am.
[89] Gabriel J.X. Dance, LaForgia, and Confessore, "Facebook Raised a Privacy Wall."
[90] Gabriel J.X. Dance, LaForgia, and Confessore.
[91] Confessore, Dance, and LaForgia, "Facebook Gave Device Makers Deep Access to Data on Users and Friends."
[92] Archibong, "Why We Disagree with The New York Times | Facebook Newsroom."
[93] Sandy Parakilas, Twitter post, June 4, 2018, 12:44 am.
[94] Gabriel J.X. Dance, Nicholas Confessore, and Michael LaForgia. "Facebook Gave Device Makers Deep Access to Dara on Users and Friends."
[95] Confessore, Dance, and LaForgia, "Facebook Gave Device Makers Deep Access to Data on Users and Friends."
[96] Confessore, Dance, and LaForgia.
[97] Confessore, Dance, and LaForgia.
[98] Confessore, Dance, and LaForgia; Wong, "Facebook Acknowledges Concerns over Cambridge Analytica Emerged Earlier than Reported."
[99] Confessore, Dance, and LaForgia, "Facebook's Device Partnerships Explained."
[100] Gabriel J.X. Dance, LaForgia, and Confessore, "Facebook Raised a Privacy Wall"; Dance, Rosenberg, and Michael, "Facebook's Data Deals Are Under Criminal Investigation."
[101] Gabriel J.X. Dance, LaForgia, and Confessore, "Facebook Raised a Privacy Wall."
[102] David Cicilline, Twitter post, June 3, 2018, 7:53 pm.
[103] Schechner and Secada, "You Give Apps Personal Information."

[104] Schechner and Secada.
[105] Anderson, "Apps Give Facebook Data."
[106] Anderson.
[107] Schechner and Secada, "You Give Apps Personal Information."
[108] Schechner and Secada.
[109] Anderson, "Apps Give Facebook Data."
[110] Schechner and Secada, "You Give Apps Personal Information."
[111] Schechner and Secada.
[112] Schechner and Secada.
[113] Reuters and Palmer, "Facebook Lawsuits Pile In."
[114] Langone, "Facebook Collecting Android Data."
[115] "Fact Check."
[116] Langone, "Facebook Collecting Android Data."
[117] Gallagher, "Facebook Scraped Call, Text Message Data for Years from Android Phones [Updated]."
[118] Dillet, "Facebook Knows Literally Everything about You."
[119] Whitney, "Google Closes $3.2 Billion Purchase of Nest."
[120] Low, "The Google Assistant Is Coming to Nest Secure."
[121] Bastone, "Google Says the Built-in Microphone It Never Told Nest Users about Was 'Never Supposed to Be a Secret."
[122] Bastone.
[123] Scott Galloway, Twitter post, February 20, 2019, 6:31 am.
[124] Electronic Privacy Information Center, "EPIC - EPIC to FTC."
[125] Eva Galperin, Twitter post, February 21, 2019, 11:17 am.
[126] "Privacy Statement."
[127] Google, "US020160260135A120160908," 120160908.
[128] Dunn, "Google Safari Workaround."
[129] "Frequently Asked Questions."
[130] Dunn, "Google Safari Workaround."
[131] "Google Will Pay $22.5 Million."
[132] O'Brien, "You Had Questions about Your Facebook Data. I Have Answers."
[133] Collins, "Google Collects Android Users' Locations Even When Location Services Are Disabled."
[134] Merriman, "Google Is Being Sued over 'privacy-Invading' Location Data Collection"; Stempel, "Lawsuit Says Google Tracks Phone Users Regardless of Privacy Settings."
[135] Accessible at https://adssettings.google.com/
[136] "Ad Personalization."
[137] "About the FTC."
[138] "About the FTC."
[139] United States Government Accountability Office, "Internet Privacy," 14.
[140] Representative James R. Langevin, "Competition and Consumer Protection."
[141] United States Government Accountability Office, "Internet Privacy," 14.
[142] Miller, "FTC Policy Statement on Deception."
[143] United States Government Accountability Office, "Internet Privacy," 10.
[144] For more see Confessore, "Audit Approved of Facebook Policies."
[145] Brookman, "Competition and Consumer Protection."

[146] Schlesinger and Andrea Day, "Most People Just Click."
[147] Zaeem, German, and Barber, "PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining," 1.
[148] United States Government Accountability Office, "Internet Privacy," 22.
[149] Representative James R. Langevin, "Competition and Consumer Protection."
[150] U.S. House, H.R.2313 - An act to amend the Federal Trade Commission Act to extend the authorization of appropriations contained in such Act, and for other purposes.
[151] Garvey, "A Brief Overview of Rulemaking and Judicial Review"; Perschuk, "Lecture III: Stoning the National Nanny: Congress and the FTC in the Late 70's,"; "The FTC as National Nanny."
[152] Dixon, "Comments of the World Privacy Forum to the Federal Trade Commission"; United States Government Accountability Office, "Internet Privacy," 12.
[153] Lubbers, "It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking," 1995.
[154] Federal Trade Commission, "Fiscal Year 2018 Agency Financial Report," 6.
[155] Ghosh and Scott, "Digital Deceit II," 36.
[156] "The Consumer Data Protection Act of 2018 Discussion Draft - Senator Wyden."
[157] Particularly in the subsection "History of Bad Behavior." Other sources are previous policy recommendations that offer broader, non-operationalized recommendations. See Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change"; Ghosh and Scott, "#Digital Deceit"; Ghosh and Scott, "Digital Deceit II"; Dixon, "Comments of the World Privacy Forum to the Federal Trade Commission"; Representative James R. Langevin, "Competition and Consumer Protection"; Brookman, "Competition and Consumer Protection"; House of Commons Digital, Culture, Media and Sport Committee, "Disinformation and 'Fake News': Final Report"; Miller, "FTC Policy Statement on Deception"; Kang, Kaplan, and Fandos, "Knowledge Gap Hinders Ability of Congress to Regulate Silicon Valley"; Solove, *Understanding Privacy*.
[158] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," 35.
[159] Public Citizen, "The Time Is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States."
[160] Information Technology & Innovation Foundation, "A Grand Bargain on Data Privacy Legislation for America."
[161] Schatz, Data Care Act of 2018.
[162] Markey, CONSENT Act.
[163] Rubio, ADD Act.
[164] Markey, Privacy Bill of Rights Act.
[165] "Schatz Leads Group of 15 Senators."
[166] "Schatz Leads Group of 15 Senators."
[167] Sec.3 (b)(1) in Schatz, Data Care Act of 2018.
[168] Sec.3 (b)(2) in Schatz.
[169] Sec.3 (b)(3) in Schatz.
[170] Sec.2 (3) in Schatz.
[171] Sec. 4(a)(1) in Schatz.
[172] The National Conference of State Legislatures maintains a database listing the relevant state laws. "Security Breach Notification Laws."
[173] Sec.3 (d)(1) in Schatz, Data Care Act of 2018.
[174] Sec.4 (a)(3) in Schatz.

[175] Sec.3 (c) in Schatz.
[176] Sec. 2(4) in Schatz.
[177] Hendrix, "Regulations Impact Small Business and the Heart of America's Economy."
[178] Baker, "One Size Fits None: The Myth of 'The Average Startup.'"
[179] Sec. 3(b)(1) in Schatz, Data Care Act of 2018.
[180] Representative James R. Langevin, "Competition and Consumer Protection."
[181] Sec. 3(b)(2)(B)(i) in Schatz, Data Care Act of 2018.
[182] Sec. 3(b)(2)(B)(ii) in Schatz.
[183] "Markey and Blumenthal Introduce Privacy Bill."
[184] "Markey and Blumenthal Introduce Privacy Bill."
[185] Sec. 2(b)(2)(B)(iii) in Markey, CONSENT Act.
[186] Sec. 2(b)(2)(B)(vii)(I) in Markey.
[187] Sec. 2(b)(2)(B)(i) in Markey.
[188] Sec. 2(b)(2)(B)(vii)(II) in Markey.
[189] Sec. 2(a)(4) in Markey.
[190] Sec. 2(b)(2)(B) in Markey.
[191] Sec. 2(b)(2)(A) in Markey.
[192] Sec. 2(b)(2)(A)(i) in Markey.
[193] Sec. 2(d) in Markey, CONSENT Act.
[194] Sec. 2(b)(2)(B)(vi) in Markey.
[195] Sec. 2(b)(2)(A) in Markey.
[196]Sec. 2(b)(2)(B)(iii) in Markey.
[197] Sec. 2(b)(2)(B) (iii) in Markey.
[198] Ebeck, "Punitive Damages: 14 Yeas Post-Campbell, Questions Remain."
[199] Ebeck.
[200] "Rubio Introduces Privacy Bill to Protect Consumers While Promoting Innovation."
[201] Sec. 3(a) in Rubio, ADD Act.
[202] Sec. 4(a)(1) in Rubio.
[203] Sec. 4(a)(2) in Rubio.
[204] Sec. 4, Sec. 4(b)(1)(C)(ii)(II), Sec. 4(b)(1)(G)-(H) in Rubio.
[205] Sec.2(a)(5) in Rubio.
[206] Electronic Privacy Information Center, "The Privacy Act of 1974"; United States Department of Justice Office of Privacy and Civil Liberties, "Overview of The Privacy Act of 1974."
[207] "Markey Introduces Privacy Legislation."
[208] "Markey Introduces Privacy Legislation."
[209] Sec. 11 in Markey, Privacy Bill of Rights Act.
[210] Sec. 13 in Markey.
[211] Sec. 4 in Markey.
[212] Sec. 12 in Markey.
[213] Sec. 16 and Sec. 17 in Markey.
[214] Sec. 13 (b)(3)(A) in Markey.
[215] Sec. 13 (b)(3)(B) in Markey.
[216] Sec. 3(b)(3) and Sec. 4(b)(3) in Markey.
[217] Sec. 4 in Markey.
[218] Sec. 4 (a)(2) in Markey.
[219] Sec. 4(a)(3)(C) in Markey.

[220] Sec. 6(a) in Markey.
[221] Sec. 6(c) in Markey.
[222] Sec. 5(a) in Markey.
[223] Sec. 12 (1) in Markey.
[224] Sec. 12(2) in Markey.
[225] Sec. 3(b)(1) in Markey.
[226] Sec. 7 and Sec. 5(a) in Markey, Privacy Bill of Rights Act.
[227] Sec. 2(3) in Markey.
[228] Sec. 13 (b)(3)(B) in Markey, Privacy Bill of Rights Act.
[229] Sec. 4 in Markey.
[230] Sec. 5 in Markey.
[231] Sec. 6 in Markey.
[232] Sec. 12 in Markey.
[233] Sec. 17 in Markey.
[234] Ebeck, "Punitive Damages: 14 Yeas Post-Campbell, Questions Remain."
[235] "Wyden Releases Discussion Draft."
[236] "Wyden Releases Discussion Draft."
[237] Sec. 6 and Sec. 7 in Wyden, Consumer Data Protection Act.
[238] Sec. 4 and Sec. 5(b)in Wyden.
[239] Sec. 6 in Wyden.
[240] Sec. 7 (b)(1) in Wyden.
[241] Sec. 8 and Sec. 9 in Wyden.
[242] Sec. 7(b)(1)(G) in Wyden.
[243] Sec. 2(12) in Wyden.
[244] Sec. 7(b)(1)(D) in Wyden, Consumer Data Protection Act.
[245] Sec. 7(b)(1)(D)-(E) in Wyden.
[246] Sec. 6(a)(1)-(11) in Wyden.
[247] Sec. 7(b)(1)(B) in Wyden, Consumer Data Protection Act.
[248] Sec. 4 in Wyden, Consumer Data Protection Act.
[249] Sec. 6(c) and Sec. 7(d)(1) in Wyden.
[250] Sec. 8 in Wyden.
[251] Sec. 9(a)(1)-(2) in Wyden.
[252] Sec. 8(d) and Sec. 9(2)(a) in Wyden.
[253] Sec. 2(5)(B)(iii) in Wyden.
[254] "NIST Mission, Vision, Core Competencies, and Core Values."
[255] Sec. 6(a)(1)(A) in Wyden, Consumer Data Protection Act.
[256] Sec. 6 (b)(10), Sec. 7(b)(1)(E), and Sec. 11(1) of Wyden.
[257] Sec. 7(b)(1)(G)-(H) in Wyden; "Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights," 5.
[258] Sec. 7(b)(3) in Wyden, Consumer Data Protection Act.
[259] Sec. 2(12) in Wyden.
[260] Sec. 6(a)(3) in Wyden.
[261] Sec. 6(b)(1)(B) in Wyden.
[262] Sec. 7(b)(1)(D) in Wyden.
[263] Sec. 4(a)(1) , Sec. 4(a)(2)(A)-(C), and Sec. 4(c) in Markey, Privacy Bill of Rights Act.

[264] Electronic Privacy Information Center, "The Gramm-Leach-Bliley Act." See Sec. 6(c) in Wyden, Consumer Data Protection Act.
[265] Sec. 3 in Wyden, Consumer Data Protection Act.
[266] "Wyden Releases Discussion Draft."
[267] General Data Protection Regulation.
[268] Hackett, "Is Big Tech Ready?"
[269] See California Consumer Privacy Act of 2018.
[270] Scott, "Europe's New Privacy Rules Are No Silver Bullet."
[271] Web Focus LLC, "U.S. Companies Projected to Spend $41.7 Bn on Compliance with the EU's GDPR Legislation."
[272] Hackett, "Is Big Tech Ready?"
[273] Davies, "GDPR Mayhem."
[274] European Data Protection Board, "First Overview of the GDPR," 8.
[275] Wolff, "How Is the GDPR Doing?"
[276] Rebecca Hill, "Year 1 of GDPR: Over 200,000 Cases Reported, Firms Fined €56 Meeelli... Oh, That's Mostly Google," The Register, March 14, 2019, https://www.theregister.co.uk/2019/03/14/more_than_200000_gdpr_cases_in_the_first_year_55m_in_fines/.
[277] Davies, "GDPR Mayhem."
[278] Seb, "A Month after GDPR Takes Effect, Programmatic Ad Spend Has Started to Recover."
[279] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," i & iv.
[280] Acxiom, "Acxiom Corporation Annual Report 2014," 2014, 8, http://www.annualreports.com/HostedData/AnnualReportArchive/a/NASDAQ_ACXM_2014.pdf.
[281] These subparts in their entirety are available at Office for Civil Rights, "HIPAA Administrative Simplification."
[282] 45 CFR § 164.506
[283] 45 CFR §§ 164.502(b), 164.514(d)
[284] 45 CFR §§ 160.103, 164.501
[285] 45 CFR §§ 160.103, 164.502(e), 164.514(e)
[286] 45 CFR § 164.502(g)
[287] 45 CFR§§ 164.501, 164.514(e)
[288] 45 CFR §§ 64.501, 164.508(f), 164.512(i)
[289] 45 CFR §§ 160.300, 164.512(b), 164.512(f)
[290] 45 CFR 164.501
[291] Office of the Assistant Secretary for Planning and Evaluation, "STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION."
[292] "Fair Credit Reporting Act: 15 U.S.C. §§ 1681-1681x."
[293] Electronic Privacy Information Center, "The Gramm-Leach-Bliley Act."
[294] 5 U.S.C § 552a(b); United States Department of Justice Office of Privacy and Civil Liberties, "Overview of The Privacy Act (2015 Edition)," 54–115.
[295]5 U.S.C §§ 552a(c)(1)-(4); United States Department of Justice Office of Privacy and Civil Liberties, 116–17.
[296] 5 U.S.C § 552a(d)(1); United States Department of Justice Office of Privacy and Civil Liberties, 118–29.

[297] 5 U.S.C §§ 552a(d)(2)-(4), 552a(c)(4); United States Department of Justice Office of Privacy and Civil Liberties, 129–30.
[298]5 U.S.C §§ 552a(e)(1)-(11); United States Department of Justice Office of Privacy and Civil Liberties, 130–66.
[299] 5 U.S.C §§ 552a(f)(1)-(5); United States Department of Justice Office of Privacy and Civil Liberties, 166–70.
[300] 5 U.S.C § 552a(g); United States Department of Justice Office of Privacy and Civil Liberties, 170–77.
[301] Sec. 2(o)(A) in Government Printing Office.
[302] Sec. 2(o)(B) in Government Printing Office.
[303] Sec. 2(o)(C) in Government Printing Office.
[304] Sec. 2(o)(D)-(I) in Government Printing Office.
[305] Sec. 2(o) (J) in Government Printing Office.
[306] Sec. 2(o) (K) in Government Printing Office.
[307] Zamora and Seckman, "FACEBOOK: TRANSPARENCY AND USE OF CONSUMER DATA," 92–95.
[308] Transcript courtesy of Bloomberg Government, "Transcript of Mark Zuckerberg's Senate Hearing."
[309] Article 2(1) in General Data Protection Regulation.
[310] Sec. 2(5)(B)(iii) in Wyden, Consumer Data Protection Act.
[311] Article 4(1) in General Data Protection Regulation.
[312] Sec. 2(12) in Wyden, Consumer Data Protection Act.
[313] Article 83(5) in General Data Protection Regulation.
[314] Sec. 4 in Wyden, Consumer Data Protection Act.
[315] Sec. 4 in General Data Protection Regulation.
[316] Sec. 7(b)(1)(C) in Wyden, Consumer Data Protection Act.
[317] Article 40 General Data Protection Regulation.
[318] Sec. 7(b)(1)(A) in Wyden, Consumer Data Protection Act.
[319] Recital 32 in General Data Protection Regulation.
[320] Sec. 6(a)(1)(A) in Wyden, Consumer Data Protection Act.
[321] Recital 39 in General Data Protection Regulation.
[322] Article 13-14 in General Data Protection Regulation.
[323] Article 15 in United Kingdom Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)," August 2, 2018, https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.
[324] Sec. 7(b)(1)(D) in Wyden, Consumer Data Protection Act.
[325] Article 16 in General Data Protection Regulation.
[326] Sec. 7(b)(1)(F) in Wyden, Consumer Data Protection Act.
[327] Article 51 and Article 57 in General Data Protection Regulation.
[328] Article 58(1)(b) in General Data Protection Regulation.

Bibliography

"About the FTC." Federal Trade Commission. Accessed March 29, 2019. https://www.ftc.gov/about-ftc.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. "The Economics of Privacy." *Journal of Economic Literature* 54, no. 2 (June 2016). https://doi.org/10.1257/jel.54.2.442.

Acxiom. "Acxiom Corporation Annual Report 2014," 2014. http://www.annualreports.com/HostedData/AnnualReportArchive/a/NASDAQ_ACXM_2014.pdf.

"Ad Personalization." Google, March 26, 2019. https://adssettings.google.com.

Anderson, Mae. "Report: Apps Give Facebook Sensitive Health and Other Data." News Outlet. Associated Press, February 22, 2019. https://www.apnews.com/a3f5a3a5663b49c4b909da1353ee03da.

Archibong, Ime. "Why We Disagree with The New York Times | Facebook Newsroom." *Facebook Newsroom* (blog), June 3, 2018. https://newsroom.fb.com/news/2018/06/why-we-disagree-with-the-nyt/.

"As Facebook CEO Zuckerberg Testifies to Congress, Senators Markey and Blumenthal Introduce Privacy Bill of Rights." U.S. Senate, April 10, 2018. https://www.markey.senate.gov/news/press-releases/as-facebook-ceo-zuckerberg-testifies-to-congress-senators-markey-and-blumenthal-introduce-privacy-bill-of-rights.

Baker, Mike. "One Size Fits None: The Myth of 'The Average Startup.'" OpenView Labs, February 12, 2016. https://labs.openviewpartners.com/one-size-fits-none-the-myth-of-the-average-startup/.

Bastone, Nick. "Google Says the Built-in Microphone It Never Told Nest Users about Was 'Never Supposed to Be a Secret." News Outlet. Business Insider, February 19, 2019. https://www.businessinsider.com/nest-microphone-was-never-supposed-to-be-a-secret-2019-2.

"Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights." Washington, DC: Executive Office of the President, May 2016. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

Brookman, Justin. "Competition and Consumer Protection in the 21st Century Hearings, Project Number P1812201," August 20, 2018. https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0052-d-0018-154961.pdf.

Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *Guardian*, March 17, 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

California Consumer Privacy Act of 2018, Pub. L. No. SB-1121, § 1798.100 (2018). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

"Carpenter v. United States." Legal Reference. Oyez, March 23, 2019. https://www.oyez.org/cases/2017/16-402.

CipherCloud. "The New Consumer Data Protection Act from Senator Ron Wyden from Oregon." *Security Boulevard* (blog), January 7, 2019. https://securityboulevard.com/2019/01/the-new-consumer-data-protection-act-from-senator-ron-wyden-from-oregon/.

Collins, Damian. Twitter post, March 21 2019, 11:01 am, https://twitter.com/DamianCollins/status/1108790827411738625.

Collins, Keith. "Google Collects Android Users' Locations Even When Location Services Are Disabled." Quartz, November 21, 2017. https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/.

Confessore, Nicholas. "Audit Approved of Facebook Policies, Even After Cambridge Analytica Leak." *New York Times*, April 19, 2018. https://www.nytimes.com/2018/04/19/technology/facebook-audit-cambridge-analytica.html.

Confessore, Nicholas, Gabriel J.X. Dance, and Michael LaForgia. "Facebook's Device Partnerships Explained." *New York Times*, June 4, 2018. https://www.nytimes.com/2018/06/04/technology/facebook-device-partnerships.html.

Confessore, Nicholas, Gabriel X.J. Dance, and Michael LaForgia. "Facebook Gave Device Makers Deep Access to Data on Users and Friends." *New York Times*, June 3, 2018. https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html?module=inline.

Cornell Law School Legal Information Institute. "Katz v. United States." University. Cornell Law School. Accessed February 19, 2019. https://www.law.cornell.edu/supremecourt/text/389/347#writing-USSC_CR_0389_0347_ZO.

CSPi. "What Is the Latest Consumer Data Protection Act That Everyone Is Talking About?" CSPi, December 13, 2018. https://www.cspi.com/consumer-data-protection-act-blog/.

Cuthbertson, Anthony. "Mark Zuckerberg Lied to Congress about Facebook Data Scandal, Congressman Claims." *Independent*, June 5, 2018. https://www.independent.co.uk/life-style/gadgets-and-tech/news/mark-zuckerberg-facebook-data-scandal-lied-congress-david-cicilline-a8384261.html.

Dance, Gabriel J.X., Matthew Rosenberg, and LaForgia Michael. “Facebook’s Data Deals Are Under Criminal Investigation.” *New York Times*, March 13, 2019. https://www.nytimes.com/2019/03/13/technology/facebook-data-deals-investigation.html.

Davies, Jessica. “GDPR Mayhem: Programmatic Ad Buying Plummets in Europe.” Digiday, May 25, 2018. https://digiday.com/media/gdpr-mayhem-programmatic-ad-buying-plummets-europe/.

Davis, Jessica. “Proposed Privacy Bill Mirrors GDPR, Adds Jail Time for Lying CEOs.” HealthcareITNews, November 2, 2018. https://www.healthcareitnews.com/news/proposed-privacy-bill-mirrors-gdpr-adds-jail-time-lying-ceos.

Dillet, Romain. “Facebook Knows Literally Everything about You.” TechCrunch, March 23, 2018. http://social.techcrunch.com/2018/03/23/facebook-knows-literally-everything-about-you/.

Dixon, Pam. “Comments of the World Privacy Forum to the Federal Trade Commission,” August 20, 2018. https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0052-d-0039-155214.pdf.

Dunn, John E. “Google Sued over IPhone ‘Safari Workaround’ Data Snooping.” naked security by Sophos, November 30, 2017. https://nakedsecurity.sophos.com/2017/11/30/google-sued-over-iphone-safari-workaround-data-snooping/.

Ebeck, Allison L. “Punitive Damages: 14 Yeas Post-Campbell, Questions Remain.” *Practical Lawyer* 63, no. 2 (April 2017): 19–I. http://search.proquest.com.ezp-prod1.hul.harvard.edu/docview/1883487966?accountid=11311.

Eggerton, John. “NCTA’s Powell: Net Neutrality Debate Is Increasingly Irrelevant.” Industry Publication. Multichannel News, March 6, 2018. https://www.multichannel.com/news/nctas-powell-net-neutrality-debate-increasingly-irrelevant-418527.

Electronic Privacy Information Center. “EPIC to FTC: After Home Spying Reports, Google Should Divest Nest,” February 20, 2019. https://epic.org/2019/02/epic-to-ftc-after-home-spying-.html.

“The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report.” EPIC, March 28, 2019. https://epic.org/privacy/fcra/#.

“The Gramm-Leach-Bliley Act.” EPIC. Accessed March 28, 2019. https://epic.org/privacy/glba/.

“The Privacy Act of 1974.” EPIC. Accessed March 27, 2019. https://epic.org/privacy/1974act/.

European Data Protection Board. “First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities.” European Parliament, February 26, 2019. http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf.

"Fact Check: Your Call and SMS History." *Facebook Newsroom* (blog), March 25, 2018. https://newsroom.fb.com/news/2018/03/fact-check-your-call-and-sms-history/.

"Fair Credit Reporting Act 15 U.S.C. § 1681." Washington, DC: Federal Trade Commission, 2018. https://www.ftc.gov/system/files/545a_fair-credit-reporting-act-0918.pdf.

"Fair Credit Reporting Act: 15 U.S.C. §§ 1681-1681x." Federal Trade Commission. Accessed March 28, 2019. https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act.

Federal Trade Commission. "Data Brokers: A Call for Transparency and Accountability." Washington, DC, May 2014. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

"Fiscal Year 2018 Agency Financial Report." Washington, DC, 2018. https://www.ftc.gov/system/files/documents/reports/agency-financial-report-fy2018/ftc_agency_financial_report_fy2018_1.pdf.

Galloway, Scott. Twitter post, February 20, 2019, 6:31 am, https://twitter.com/profgalloway/status/1098228685155508224?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1098228685155508224&ref_url=https%3A%2F%2Fwww.washingtonpost.com%2Fbusiness%2F2019%2F02%2F20%2Fgoogle-forgot-notify-customers-it-put-microphones-nest-security-systems%2F

Galperin, Eva. Twitter post, February 21, 2019, 11:17 am, https://twitter.com/evacide/status/1098663007079395328.

Parakila, Sandy. Twitter post, June 4, 2018, 12:44 am, https://twitter.com/mixblendr/status/1003542893171302406.

Parakila, Sandy. Twitter post, June 4, 2018, 12:44 am, https://twitter.com/mixblendr/status/1003542900532240384.

Parakila, Sandy. Twitter post, June 4, 2018, 12:44 am, https://twitter.com/mixblendr/status/1003542902247772161.

"Preliminary FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change." Policy Report. Washington, DC, December 2010. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

"Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers." Policy Report. Washington, DC, March 2012. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

"Frequently Asked Questions." Google You Owe Us. Accessed March 26, 2019. https://www.youoweus.co.uk/faqs/.

Gabriel J.X. Dance, Michael LaForgia, and Nicholas Confessore. "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants." *New York Times*, December 18, 2018. https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html#click=https://t.co/p565d1TX5L.

Gallagher, Sean. "Facebook Scraped Call, Text Message Data for Years from Android Phones [Updated]." News Outlet. Ars Technica, March 24, 2018. https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-from-android-phones/.

Garvey, Todd. "A Brief Overview of Rulemaking and Judicial Review." Washington, DC: Congressional Research Service, March 27, 2017. https://fas.org/sgp/crs/misc/R41546.pdf.

General Data Protection Regulation, Pub. L. No. L 119/1, Regulation (EU) 2016/679 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

Ghosh, Dipayan, and Ben Scott. "Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet." Policy Report. Harvard Shorenstein Center on Media, Politics, and Public Policy, September 2018. https://shorensteincenter.org/wp-content/uploads/2018/09/Digital_Deceit_2_Final.pdf?x78124.

"#Digital Deceit: The Technologies Behind Precision Propaganda on the Internet." Policy Report. Harvard Shorenstein Center on Media, Politics, and Public Policy, January 2018. https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/.

Google. "US020160260135A120160908." United States Patent and Trademark Office. http://pdfaiw.uspto.gov/.aiw?docid=20160260135&PageNum=7&IDKey=4821DA74E311&HomeUrl=http://appft.uspto.gov/netacgi/nph-Parser?Sect1.

"Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser." Federal Trade Commission, August 9, 2012. https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

Government Printing Office, Pub. L. No. 100–503 (1988). https://www.govinfo.gov/content/pkg/STATUTE-102/pdf/STATUTE-102-Pg2507.pdf.

Gramlich, John. "10 Facts about Americans and Facebook." Fact Tank. Pew Research Center, February 1, 2019. http://www.pewresearch.org/fact-tank/2019/02/01/facts-about-americans-and-facebook/.

Green, Andy. "Wyden's Consumer Data Protection Act: How to Be Compliant." Varonis, January 1, 2019. https://www.varonis.com/blog/gdpr-american-style-preview-of-federal-us-privacy-law-part-ii/.

Hackett, Robert. “Sen. Wyden Proposed a CEO-Felling Data Privacy Law. Is Big Tech Ready for It?” Fortune, November 3, 2018. http://fortune.com/2018/11/03/privacy-law-tech-ceo-wyden/.

Harvard Institute of Politics. *Big Tech and Democracy*. YouTube Video, 2019. https://www.youtube.com/watch?v=HbVYpP4gWAQ.

Hendrix, Michael. “Regulations Impact Small Business and the Heart of America’s Economy.” U.S. Chamber of Commerce Foundation, March 14, 2017. https://www.uschamberfoundation.org/blog/post/regulations-impact-small-business-and-heart-americas-economy.

Hern, Alex. “Facebook: Washington DC Sues Tech Giant over Cambridge Analytica Data Use.” *Guardian*, December 19, 2018. https://www.theguardian.com/technology/2018/dec/19/facebook-cambridge-analytica-washington-dc-lawsuit-data.

Hill, Rebecca. “Year 1 of GDPR: Over 200,000 Cases Reported, Firms Fined €56 Meeelli... Oh, That’s Mostly Google.” The Register, March 14, 2019. https://www.theregister.co.uk/2019/03/14/more_than_200000_gdpr_cases_in_the_first_year_55m_in_fines/.

Hitlin, Paul, and Lee Rainie. “Facebook Algorithms and Personal Data.” Pew Research Center, January 16, 2019. https://www.pewInternet.org/2019/01/16/facebook-algorithms-and-personal-data/.

Hoofnagle, Chris Jay, and Jan Whittington. “Free: Accounting for the Costs of the Internet’s Most Popular Price.” *UCLA Law Review* 61, no. 3 (February 2014).

House of Commons Digital, Culture, Media and Sport Committee. “Disinformation and ‘Fake News’: Final Report.” Government Report. London, UK: House of Commons, 2019. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

Igo, Sarah E. *The Known Citizen*. Cambridge, MA: Harvard University Press, 2018.

Information Technology & Innovation Foundation. “A Grand Bargain on Data Privacy Legislation for America,” January 14, 2019. https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america.

Kang, Cecilia, Thomas Kaplan, and Nicholas Fandos. “Knowledge Gap Hinders Ability of Congress to Regulate Silicon Valley.” *New York Times*, April 12, 2018. https://www.nytimes.com/2018/04/12/business/congress-facebook-regulation.html.

“Katz v. United States, 389 U.S. 347 (1967).” Legal Reference. Justia. Accessed February 19, 2019. https://supreme.justia.com/cases/federal/us/389/347/.

Kerry, Cameron F. “Will This New Congress Be the One to Pass Data Privacy Legislation?” Brookings Institute, January 7, 2019. https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/.

Kozlowska, Hanna. “The Cambridge Analytica Scandal Affected Nearly 40 Million More People than We Thought.” Quartz, April 4, 2018. https://qz.com/1245049/the-cambridge-analytica-scandal-affected-87-million-people-facebook-says/.

Langone, Alix. “Facebook Has Been Collecting Android Users’ Cell Phone Data For Years.” *Time*, March 26, 2018. http://time.com/5215274/facebook-messenger-android-call-text-message-data/.

Low, Erick. “The Google Assistant Is Coming to Nest Secure.” *Google* (blog), February 4, 2019. https://www.blog.google/products/assistant/nest-secure-google-assistant/.

Lubbers, Jeffery S. “It’s Time to Remove the ‘Mossified’ Procedures for FTC Rulemaking.” *George Washington Law Rewiew* 83, no. 6 (2015). http://www.gwlr.org/wp-content/uploads/2016/01/83-Geo-Wash-L-Rev-1979.pdf.

Madden, Mary, and Lee Rainie. “Americans’ Attitudes About Privacy, Security and Surveillance.” Fact Tank. Pew Research Center, May 20, 2015. https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Markey, Edward J. CONSENT Act, Pub. L. No. S.2639 (2018). https://www.congress.gov/bill/115th-congress/senate-bill/2639/text.

Privacy Bill of Rights Act, Pub. L. No. OLL19313 (2019). https://www.markey.senate.gov/imo/media/doc/Privacy%20Bill%20of%20Rights%20Act.pdf.

Merriman, Chris. “Google Is Being Sued over ‘privacy-Invading’ Location Data Collection.” The Inquirer, August 21, 2018. https://www.theinquirer.net/inquirer/news/3061399/google-is-being-sued-over-privacy-invading-location-data-collection.

Miller, James C. “FTC Policy Statement on Deception,” October 14, 1983. https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf .

Narayanan, Arvind. “Privacy and the Market for Lemons, or How Websites Are Like Used Cars.” *33 Bits of Entropy* (blog), March 18, 2011. https://33bits.wordpress.com/2011/03/18/privacy-and-the-market-for-lemons-or-how-websites-are-like-used-cars/.

“NIST Mission, Vision, Core Competencies, and Core Values.” NIST, January 26, 2017. https://www.nist.gov/about-nist/our-organization/mission-vision-values.

O’Brien, Sara Ashley. “You Had Questions about Your Facebook Data. I Have Answers.” CNN Money, March 27, 2018. https://money.cnn.com/2018/03/27/technology/facebook-data-questions/index.html.

Office for Civil Rights. “HIPAA Administrative Simplification: Regulation Text.” Washington, DC: U.S. Department of Health and Human Services, March 2013. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf?language=es.

Office of the Assistant Secretary for Planning and Evaluation. “STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.” U.S. Department of Health & Human Services, July 6, 2001. https://aspe.hhs.gov/standards-privacy-individually-identifiable-health-information.

Perschuk, Michael. “Lecture III: Stoning the National Nanny: Congress and the FTC in the Late 70’s,” https://www.ftc.gov/system/files/documents/public_statements/688981/19811104_pertschuk_lecture_iii_stoning_the_national_nanny-_congress_and_the_ftc_in_the_late_70s.pdf.

Pound, Roscoe. “Interests of Personality.” Harvard Law Review 28, no. 5 (1915). https://doi.org/10.2307/1326270.

Privacy Protection Study Commission. “Personal Privacy in an Information Society: The Report of The Privacy Protection Study Commission.” Washington, DC: Government Printing Office, 1977. https://www.ncjrs.gov/pdffiles1/Digitization/49602NCJRS.pdf.

“Privacy Statement for Nest Products and Services.” Technology. Nest, September 24, 2018. https://nest.com/legal/privacy-statement-for-nest-products-and-services/.

Public Citizen. “The Time Is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States.” Policy Report, April 11, 2019. https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf.

Rainie, Lee. “How Americans Feel about Social Media and Privacy.” Fact Tank. Pew Research Center, March 27, 2018. https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

Rampell, Catherine. “Opinion | Our Politicians Have No Idea How the Internet Works.” *Washington Post*, August 20, 2018. https://www.washingtonpost.com/opinions/how-can-congress-police-the-internet-when-they-dont-even-understand-it/2018/08/20/46f6baa6-a4b4-11e8-97ce-cc9042272f07_story.html.

Reagan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill, N.C.: University of North Carolina Press, 1995.

Representative James R. Langevin. Response to FTC request for comment. “Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201.” Response to FTC request for comment, August 20, 2018. https://www.ftc.gov/system/files/filings/initiatives/758/public_comment_from_representative_langevin_re_topic_5_redacted.pdf.

Reuters, and Annie Palmer. “First Lawsuits Begin to Pile in over Facebook Data Collection as Three Users SUE the Firm Seeking Class Action Status after It Admitted It Logged Calls and Texts from Android Devices.” News Outlet. DailyMail, March 27, 2018. https://www.dailymail.co.uk/sciencetech/article-5551933/Three-Facebook-users-sue-collection-call-text-history.html.

Ribak, Rivka. “‘Privacy Is a Basic American Value:’ Globalization and the Construction of Web Privacy in Israel.” *The Communication Review* 10, no. 1 (2007).

Rosenberg, Matthew, Nicholas Confessore, and Carole Cadwalladr. “How Trump Consultants Exploited the Facebook Data of Millions.” *New York Times*, March 17, 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Rothman, Lily. “The Surprising History Behind America’s Stand Your Ground Laws.” *Time*, February 15, 2017. http://time.com/4664242/caroline-light-stand-your-ground-qa/.

“Rubio Introduces Privacy Bill to Protect Consumers While Promoting Innovation.” U.S. Senate, January 16, 2019. https://www.rubio.senate.gov/public/index.cfm/2019/1/rubio-introduces-privacy-bill-to-protect-consumers-while-promoting-innovation.

Rubio, Marco. ADD Act, Pub. L. No. S,142 (2019). https://www.congress.gov/bill/116th-congress/senate-bill/142.

Rule Making, 5 U.S.C. § 553. https://www.law.cornell.edu/uscode/text/5/553.

Schatz, Brian. Data Care Act of 2018, Pub. L. No. S.3744 (2018). https://www.congress.gov/bill/115th-congress/senate-bill/3744.

“Schatz Leads Group of 15 Senators In Introducing New Bill To Help Protect People’s Personal Data Online.” U.S. Senator Brian Schatz of Hawaii, December 12, 2018. https://www.schatz.senate.gov/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online.

Schechner, Sam, and Mark Secada. “You Give Apps Sensitive Personal Information. Then They Tell Facebook.” *Wall Street Journal*, February 22, 2019. https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636?mod=hp_lead_pos1.

Schlesinger, Jennifer, and Andrea Day. “Most People Just Click and Accept Privacy Policies without Reading Them — You Might Be Surprised at What They Allow Companies to Do.” News Outlet. CNBC, March 15, 2019. https://www.cnbc.com/2019/02/07/privacy-policies-give-companies-lots-of-room-to-collect-share-data.html.

Scott, Mark. “Europe’s New Privacy Rules Are No Silver Bullet.” Politico, April 28, 2018. https://www.politico.eu/article/gdpr-rules-europe-facebook-data-protection-privacy-general-data-protection-regulation-cambridge-analytica/.

Seb, Joseph. “A Month after GDPR Takes Effect, Programmatic Ad Spend Has Started to Recover.” Digiday, June 25, 2018. https://digiday.com/marketing/month-gdpr-takes-effect-programmatic-ad-spend-started-recover/A month after GDPR takes effect, programmatic ad spend has started to recover.

“Security Breach Notification Laws.” National Conference of State Legislatures, September 28, 2018. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

Senate Committee on Government Operations, and House Committee on Government Operation. “Legislative History of the Privacy Act of 1974, S. 3418 (Public Law 93-579).” Legislative History. Washington, DC, 1976. https://congressional-proquest-com.ezp-prod1.hul.harvard.edu/congressional/result/pqpresultpage.gispdfhitspanel.pdflink/$2fapp-bin$2fgis-congresearch$2f4$2f0$2f9$2f1$2fcmp-1976-ops-0021_from_1_to_1470.pdf/entitlementkeys=1234%7Capp-gis%7Ccongresearch%7Ccmp-1976-ops-0021.

“Senator Markey Introduces Comprehensive Privacy Legislation.” U.S. Senate, April 12, 2019. https://www.markey.senate.gov/news/press-releases/senator-markey-introduces-comprehensive-privacy-legislation.

Sluis, Sarah. “Digital Ad Market Soars To $88 Billion, Facebook And Google Contribute 90% Of Growth.” AdExchanger, May 10, 2018. https://adexchanger.com/online-advertising/digital-ad-market-soars-to-88-billion-facebook-and-google-contribute-90-of-growth/.

Solove, Daniel J. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.

Stempel, Jonathan. “Lawsuit Says Google Tracks Phone Users Regardless of Privacy Settings.” Reuters, August 20, 2018. https://www.reuters.com/article/us-alphabet-google-privacy-lawsuit-idUSKCN1L51M3.

“The Consumer Data Protection Act of 2018 Discussion Draft - Senator Wyden.” U.S. Senate. Accessed April 16, 2019. https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20one%20pager%20Nov%201.pdf.

“The Digital Advertising Stats You Need for 2018.” Marketing Data. AppNexus, March 7, 2018.

“The FTC as National Nanny,” March 1, 1978. https://www.washingtonpost.com/archive/politics/1978/03/01/the-ftc-as-national-nanny/69f778f5-8407-4df0-b0e9-7f1f8e826b3b/?noredirect=on&utm_term=.34f9560acff3.

“The State of Privacy in Post-Snowden America.” Fact Tank. Pew Research Center, September 21, 2016. http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

"The Top 500 Sites on the Web." Alexa. Accessed March 25, 2018. https://www.alexa.com/topsites.

Transcript courtesy of Bloomberg Government. "Transcript of Mark Zuckerberg's Senate Hearing." *Washington Post*, April 10, 2018. https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.9120f04d8ec6.

Tsukayama, Hayley. "Alphabet Shares Soar despite Hit to Profit from Google's European Union Fine." *Washington Post*, July 23, 2018. https://www.washingtonpost.com/technology/2018/07/23/alphabet-shares-soar-despite-hit-profit-googles-eu-fine/.

Turley, Jonathan. "Supreme Court's GPS Case Asks: How Much Privacy Do We Expect?" *Washington Post*, November 11, 2011. https://www.washingtonpost.com/opinions/supreme-courts-gps-case-asks-how-much-privacy-do-we-expect/2011/11/10/gIQAN0RzCN_story.html?noredirect=on&utm_term=.cd9f95a9e64b.

United Kingdon Information Commissioner's Office. "Guide to the General Data Protection Regulation (GDPR)," August 2, 2018. https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

United States Department of Justice Office of Privacy and Civil Liberties. "Overview of The Privacy Act of 1974." United States Department of Justice, July 27, 2015. https://www.justice.gov/opcl/introduction.

"Overview of The Privacy Act of 1974: Policy Objectives." United States Department of Justice, July 16, 2015. https://www.justice.gov/opcl/policy-objectives.

"Privacy Act of 1974," July 17, 2015. https://www.justice.gov/opcl/privacy-act-1974 https://www.justice.gov/opcl/privacy-act-1974.

"United States Department of Justice Overview of The Privacy Act of 1974 (2015 Edition)." United States Department of Justice, 2015. https://www.justice.gov/opcl/file/793026/download.

United States Government Accountability Office. "Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility." Policy Report. Washington, DC, 2019. https://www.gao.gov/assets/700/696437.pdf.

U.S. House. H.R. 5835- Omnibus Budget Reconciliation Act of 1990, Pub. L. No. 101–508 (1990). https://www.congress.gov/bill/101st-congress/house-bill/5835/text?q=%7B%22search%22%3A%5B%22cite%3APL101-508%22%5D%7D&r=1&s=1.

H.R.2313 - An act to amend the Federal Trade Commission Act to extend the authorization of appropriations contained in such Act, and for other purposes, Pub. L. No. 96–252 (1980). https://www.congress.gov/bill/96th-congress/house-bill/2313.

H.R.3103 - Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191 (1996). https://www.congress.gov/bill/104th-congress/house-bill/3103.

U.S. Senate. S.496- Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100–503 (1988). https://www.congress.gov/bill/100th-congress/senate-bill/496.

S.900 - Gramm-Leach-Bliley Act, Pub. L. No. 106–434 (1999). https://www.congress.gov/bill/106th-congress/senate-bill/900.

S.3418 - An Act to amend title 5, United States Code, by adding a section 552a, to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes, Pub. L. No. 93–579, 5 U.S.C § 552a (1974). https://www.congress.gov/bill/93rd-congress/senate-bill/3418.

U.S. Small Business Administration. "2018 Small Business Profile," 2018. https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890).

Web Focus LLC. "U.S. Companies Projected to Spend $41.7 Bn on Compliance with the EU's GDPR Legislation." Cision, May 16, 2018. https://www.prnewswire.com/news-releases/us-companies-projected-to-spend-417-bn-on-compliance-with-the-eus-gdpr-legislation-682812501.html.

Wessler, Nathan Freed. "The Supreme Court's Groundbreaking Privacy Victory for the Digital Age." Nonprofit. American Civil Liberties Union, June 22, 2018. https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age.

Wex Legal Dictionary. "Fourth Amendment." University. Cornell Law School. Accessed February 19, 2019. https://www.law.cornell.edu/constitution/fourth_amendment.

"Privacy." University. Cornell Law School. Accessed February 19, 2019. https://www.law.cornell.edu/wex/privacy.

"What Is HIPAA?" Professional Association. American Society of Anesthesiologists. Accessed April 5, 2019. https://www.healthmedlink.com/sitex/hssbilling/hipaa.htm.

Whitney, Lance. "Google Closes $3.2 Billion Purchase of Nest." CNet, February 12, 2014. https://www.cnet.com/news/google-closes-3-2-billion-purchase-of-nest/.

Wolff, Josephine. “How Is the GDPR Doing?” Slate, March 20, 2019. https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html.

Wong, Julia Carrie. “Facebook Acknowledges Concerns over Cambridge Analytica Emerged Earlier than Reported.” *Guardian*, March 21, 2019, sec. UK news. https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing.

“Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans’ Privacy.” U.S. Senate, November 1, 2018. https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy.

Wyden, Ron. Consumer Data Protection Act, Pub. L. No. SIL18B29 (2018). https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf.

Zaeem, Razieh Nokhbeh, Rachel L German, and K. Suzanne Barber. “PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining.” *ACM Transactions on Internet Technology* 18, no. 4 (2018).

Zamora, and Seckman. “FACEBOOK: TRANSPARENCY AND USE OF CONSUMER DATA.” Washington, DC: House of Representatives Committee on Energy and Commerce, April 11, 2018. https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Transcript-20180411.pdf.